

User's Manual

VDL-2420MR
VDL-2420MR48
24-Port VDSL2 IP DSLAM



Trademarks

Copyright © PLANET Technology Corp. 2010.

Contents subject to which revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at whose own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the power cable to disconnect the device from the power circuit.

Without removing power cable, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET 24-Port VDSL2 IP DSLAM User's Manual

FOR MODELS: VDL-2420MR / VDL-2420MR48

REVISION: 1.0 (JULY.2010)

Part No.: 2080-AC0280-000

TABLE OF CONTENTS

1. INTRODUCTION	19
1.1 Package Contents	19
1.2 Product Description.....	20
1.3 How to Use This Manual.....	21
1.4 Product Features.....	22
1.5 Product Specification	25
2. INSTALLATION.....	29
2.1 Hardware Description	29
2.1.1 DSLAM Front Panel	29
2.1.2 LED Indications	31
2.1.3 IP DSLAM Rear Panel.....	33
2.2 Install the IP DSLAM	35
2.2.1 Rack Mounting.....	35
2.2.2 Installing the SFP transceiver	37
2.3 Wiring for VDSL2 Ports	39
3. DSLAM MANAGEMENT	41
3.1 Requirements	41
3.2 Management Access Overview	42
3.3 Web Management.....	43
3.4 SNMP-Based Network Management	44
3.5 Administration Console.....	44
3.6 Protocols.....	46
3.6.1 Virtual Terminal Protocols.....	46
3.6.2 SNMP Protocol.....	46
3.6.3 Management Architecture	46
4. WEB-BASED MANAGEMENT.....	47
4.1 About Web-based Management	47
4.1.1 Requirements.....	48
4.1.2 Logging on the IP DSLAM	48
4.1.3 Main WEB PAGE.....	50
4.2 System.....	51
4.2.1 System Information	52
4.2.1.1 Basic.....	52

4.2.1.2 Misc Config.....	53
4.2.1.3 Module Info	54
4.2.2 IP Configuration.....	56
4.2.3 Console Information.....	58
4.2.4 SNMP Configuration.....	58
4.2.4.1 SNMP Overview	58
4.2.4.2 System Options.....	59
4.2.4.3 Community Strings	60
4.2.4.4 Trap Managers.....	61
4.2.4.5 SNMPv3 Groups	61
4.2.4.6 SNMPv3 View	62
4.2.4.7 SNMPv3 Access	63
4.2.4.8 SNMP V3 usm-user	64
4.2.5 Syslog Setting.....	66
4.2.6 SNTP Setting.....	67
4.2.7 Firmware Upgrade	68
4.2.7.1 TFTP Firmware Upgrade	68
4.2.7.2 HTTP Firmware Upgrade	69
4.2.8 Configuration Backup.....	70
4.2.8.1 TFTP Restore Configuration	70
4.2.8.2 HTTP Config File Restore.....	71
4.2.8.3 TFTP Backup Configuration	71
4.2.8.4 HTTP Config File Backup.....	72
4.2.9 Factory Default.....	73
4.2.10 System Reboot.....	73
4.3 Port Configuration	74
4.3.1 Port Control.....	74
4.3.2 Port Status.....	76
4.3.3 Port Statistics.....	76
4.3.4 Port Sniffer	77
4.3.5 Protect Port	79
4.4 VLAN configuration	80
4.4.1 VLAN Overview	80
4.4.2 Static VLAN Configuration	83
4.4.3 Port-based VLAN	84
4.4.4 802.1Q VLAN.....	86

4.4.4.1	VLAN Group Configuration	87
4.4.4.2	VLAN Filter	91
4.4.4.3	IEEE 802.1Q Symmetric VLAN Configuration Example	92
4.4.4.4	IEEE 802.1Q VLAN Trunk Configuration Example	98
4.4.4.5	IEEE 802.1Q Overlapping VLAN Configuration Example	104
4.4.4.6	Port Trunk + IEEE 802.1Q VLAN Trunk Configuration Example	109
4.4.5	Q-in-Q VLAN	115
4.4.5.1	Q-in-Q Port Setting	116
4.4.5.2	Q-in-Q Tunnel Setting	117
4.4.6	GVRP VLAN	118
4.4.6.1	GVRP Setting	119
4.4.6.2	GVRP Table	120
4.5	Trunking	121
4.5.1	Aggregator setting	121
4.5.2	Aggregator Information	122
4.5.3	State Activity	126
4.6	Forwarding and Filtering	127
4.6.1	Dynamic MAC Table	127
4.6.2	Static MAC Table	128
4.6.3	MAC Filtering	129
4.7	IGMP Snooping	130
4.7.1	Theory	130
4.7.2	IGMP Configuration	134
4.8	Spanning Tree Protocol	135
4.8.1	Theory	135
4.8.2	Illustration of STP	138
4.8.3	STP Parameters	139
4.8.4	STP System Configuration	141
4.8.5	Port Configuration	144
4.9	DHCP Relay & Option 82	146
4.10	LLDP	148
4.10.1	LLDP Configuration	148
4.10.2	PerPort Configuration	149
4.11	Access Control List	150
4.12	Security Manager	154
4.13	MAC Limit	154

4.13.1	MAC Limit Configuration	154
4.13.2	MAC Limit Port Status.....	156
4.14	802.1x Configuration.....	157
4.14.1	Understanding IEEE 802.1x Port-Based Authentication	157
4.14.2	System Configuration	160
4.14.3	802.1x Port Configuration.....	162
4.14.4	Misc Configuration	163
4.15	QoS Configuration	164
4.15.1	Understand QoS	164
4.15.2	QoS Configuration.....	165
4.15.2.1	Priority Queue Service settings.....	165
4.15.2.2	QoS PerPort Configuration	167
4.15.3	TOS/DSCP	168
4.15.3.1	TOS/DSCP Configuration	169
4.15.3.2	TOS/DSCP Port Configuration.....	170
4.16	VDSL Configuration.....	171
4.16.1	Profile Management	171
4.16.1.1	Line Template	172
4.16.1.2	Line Profile.....	173
4.16.1.3	Channel Profile.....	176
4.16.1.4	Misc. Features	177
4.16.1.5	Alarm Template	185
4.16.1.6	Line Alarm Profile	186
4.16.1.7	Line Alarm Profile	187
4.16.2	Port Management	188
4.16.2.1	Setup	188
4.16.2.2	Status	189
4.16.3	How to Setup VDSL.....	191
4.16.3.1	Line Template and Profile Setup Example	191
4.16.3.2	Alarm Template and Profile Setup Example	195
4.16.3.3	Port Setup Example	199
5.	CONSOLE MANAGEMENT	201
5.1	Login in the Console Interface	201
5.2	Configure IP address	202
5.3	Commands Level	204
6.	COMMAND LINE INTERFACE	205

6.1 Operation Notice	205
6.2 System Commands.....	206
show running-config.....	206
copy running-config startup-config	206
erase startup-config.....	206
clear arp	206
show arp.....	206
ping.....	206
syslog-server	207
[no] sntp.....	207
sntp.....	207
6.3 DSLAM Static Configuration	208
6.3.1 Port Configuration and show status	208
port state	208
port nego.....	208
port speed.....	208
port flow	208
port rate.....	209
port priority.....	209
port jumboframe.....	209
show port status	209
show port statistics	210
show port protection	211
6.4 Trunk Configuration.....	212
6.4.1 Trunking Commands.....	212
show trunks	212
trunk add.....	212
no trunk.....	212
6.4.2 LACP Command	213
[no] lacp	213
lacp system-priority	213
no lacp system-priority.....	213
show lacp status	213
show lacp.....	214
show lacp agg	214
show lacp port.....	214

6.5 VLAN Configuration	215
6.5.1 Virtual LANs	215
6.5.2 VLAN Mode: Port-based	216
show vlan mode	216
vlan mode.....	216
6.5.3 Advanced 802.1Q VLAN Configuration	217
show vlan mode	217
vlan mode.....	217
vlan add.....	217
no vlan.....	218
show vlan.....	218
show vlan static	218
show vlan pvid	218
vlan filter	219
show vlan filter	219
6.6 Misc Configuration	220
[no] mac-age-time	220
show mac-age-time.....	220
broadcast	220
broadcast select.....	220
Collision-Retry.....	221
6.7 Administration Configuration	221
6.7.1 Change Username / Password	221
hostname	221
no hostname.....	221
[no] password.....	221
6.7.2 IP Configuration	222
ip address	222
ip default-gateway.....	222
show ip.....	222
show info.....	222
dhcp.....	223
show dhcp.....	223
6.7.3 Reboot DSLAM	223
boot.....	223
6.7.4 Reset to Default	223

erase startup-config.....	223
6.7.5 TFTP Update Firmware	223
copy tftp firmware	223
6.7.6 Restore Configure File	223
copy tftp <running-config flash>.....	223
6.7.7 Backup Configure File	224
copy <running-config flash> tftp.....	224
6.8 MAC limit.....	224
mac-limit.....	224
no mac-limit	224
mac-limit.....	225
show mac-limit	225
6.9 Port Mirroring Configuration.....	225
mirror-port.....	225
show mirror-port	225
6.10 Quality of Service.....	226
6.10.1 QoS Configuration.....	226
qos priority	226
qos level	227
show qos.....	227
6.10.2 Per Port Priority	227
port priority	227
6.11 MAC Address Configuration.....	228
clear mac-address-table	228
mac-address-table static.....	228
no mac-address-table static mac-addr	228
show mac-address-table	228
show mac-address table static.....	228
show mac-address-table multicast	228
smac-address-table static.....	229
show smac-address-table	229
show smac-address-table multicast	229
[no] filter.....	229
show filter	229
6.12 STP/MSTP Commands.....	230
[no] spanning-tree.....	230

spanning-tree forward-delay.....	230
spanning-tree hello-time	230
spanning-tree maximum-age	230
spanning-tree priority	231
show spanning-tree	231
show spanning-tree port	231
spanning-tree protocol-version.....	231
spanning-tree max-hops	231
spanning-tree name	232
spanning-tree revision.....	232
spanning-tree port path-cost	232
spanning-tree port priority	232
[no] spanning-tree port mcheck	233
[no] spanning-tree port edge-port.....	233
[no] spanning-tree port non-stp	233
spanning-tree port point-to-point-mac	233
spanning-tree mst	233
spanning-tree mst <0-15> vlan [<vlan-list>].....	234
spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]	234
spanning-tree mst <0-15> port priority <0-240> [<port-list>]	234
no spanning-tree mst.....	234
show spanning-tree	235
show spanning-tree port	235
show spanning-tree mst configuration.....	235
show spanning-tree mst <0-15>	235
show spanning-tree mst <0-15> port <1-10>.....	235
show vlan spanning-tree.....	236
6.13 SNMP	237
6.13.1 System Options	237
[no] snmp.....	237
show snmp status.....	237
snmp system-name.....	237
snmp system-location	237
snmp system-contact	237
show snmp system	238
6.13.2 Community Strings	238

snmp community	238
no snmp community	238
show snmp community	238
6.13.3 Trap Managers	238
snmp trap	238
no snmp trap	239
show snmp trap	239
6.14 IGMP	239
[no] igmp	239
[no] igmp fastleave	239
[no] igmp querier	240
[no] igmp CrossVLAN	240
show igmp	240
igmp clear_statistics	240
6.15 802.1x Protocol	241
[no] dot1x	241
radius-server host	241
radius-server key	241
radius-server nas	241
show radius-server	241
dot1x timeout quiet-period	242
dot1x timeout tx-period	242
dot1x timeout supplicant	242
dot1x timeout radius-server	242
dot1x max-req	242
dot1x timeout re-authperiod	243
show dot1x	243
dot1x port	243
show dot1x port	243
6.16 Access Control List	244
6.16.1 IPv4 ACL commands	244
no acl	244
no acl count	244
show acl	244
acl (add edit) <1-220> (permit deny) <0-4094> ipv4 <0-255>	245
acl add <1-220> (qosvoip) <0-4094>	245

6.16.2 Non-IPv4 ACL commands.....	246
acl add <1-220> (permit deny) <0-4094> nonipv4 <0-65535>.....	246
6.17 Binding	247
6.17.1 SIP/SMAC binding commands	247
bind.....	247
no bind	247
no bind	247
show bind.....	247
bind add	248
6.18 DHCP Configuration	249
[no] dhcp-option82.....	249
dhcp-option82	249
[no] dhcp-relay	249
dhcp-relay	249
dhcp-router	249
6.19 VDSL2 Commands.....	250
6.19.1 VDSL2 interface Commands	250
profile line-template	250
profile line-template new	250
profile line-template del.....	250
profile line-template set.....	251
profile line-template show.....	251
profile line-template show sprofile.....	251
profile line-template show line-template	252
profile line-template show line-profile	253
profile line-template show chan-profile	253
profile line-template show alarm-template	253
profile line-template show line-alarm-profile	253
profile line-template show port.....	254
profile line-template show virtual-noise	254
profile line-template show dpbopsd	254
profile line-template show rfi-bands	254
profile line-template show psd	254
profile line-profile.....	255
profile line-profile new	255
profile line-profile del.....	255

profile line-profile show.....	255
profile line-profile show.....	255
profile line-profile show sprofile	256
profile line-profile show line-profile	257
profile line-profile show chan-profile.....	257
profile line-profile show alarm-template.....	257
profile line-profile show line-alarm-profile	258
profile line-profile show port.....	258
profile line-profile show virtual-noise	258
profile line-profile show dpbopsd	258
profile line-profile show rfi-bands	258
profile line-profile show psd	259
profile line-profile set.....	259
profile line-profile set sys.....	259
profile line-profile set bnd	259
profile line-profile set vns	260
profile line-profile set psd	260
profile line-profile set rfi	260
profile line-profile set DPB	260
profile line-profile set profiles.....	261
profile line-profile set targetSnrmDs.....	261
profile line-profile set targetSnrmUs.....	261
profile line-profile set maxSnrmDs	261
profile line-profile set maxSnrmUs	262
profile line-profile set minSnrmDs	262
profile line-profile set minSnrmUs	262
profile line-profile set led	262
profile line-profile set bitSwapUs	263
profile line-profile set bitSwapDs	263
profile line-profile set us0disable.....	263
profile line-profile set handshakeTone	263
profile line-profile set upboKLF.....	264
profile line-profile set upboPsdA0	264
profile line-profile set upboPsdB0	264
profile line-profile set upboPsdA1	264
profile line-profile set upboPsdB1	265

profile line-profile set upboPsdA2	265
profile line-profile set upboPsdB2	265
profile line-profile set upboPsdA3	265
profile line-profile set upboPsdB3	266
profile line-profile set dpboEsEL.....	266
profile line-profile set dpboEsCableModelA	266
profile line-profile set dpboEsCableModelB	266
profile line-profile set dpboEsCableModelC	267
profile line-profile set dpboMus	267
profile line-profile set dpboFMin	267
profile line-profile set bpboFMax	267
profile line-profile set raModeDs	268
profile line-profile set raModeUs	268
profile line-profile set raUsNrmDs.....	268
profile line-profile set raUsNrmUs.....	268
profile line-profile set raUsTimeDs	269
profile line-profile set raUsTimeUs	269
profile line-profile set snrModeDs.....	269
profile line-profile set snrModeUs.....	269
profile line-profile set maxNomAtpDs.....	270
profile line-profile set maxNomAtpUs.....	270
profile line-profile set maxNomPsdDs	270
profile line-profile set maxNomPsdUs	270
profile chanprofile.....	271
profile chanprofile show sprofile	271
profile chanprofile show line-template	271
profile chanprofile show line-profile	271
profile chanprofile show chan-profile.....	271
profile chanprofile show alarm-template.....	272
profile chanprofile show line-alarm-profile	272
profile chanprofile show chan-alarm-profile	272
profile chanprofile show port.....	272
profile chanprofile show virtual-noise	272
profile chanprofile show dpbopsd	273
profile chanprofile show rfi-bands	273
profile chanprofile show psd	273

profile alarm-template.....	273
profile alarm-template show sprofile	274
profile alarm-template show line-profile.....	275
profile alarm-template show chan-profile.....	275
profile alarm-template show alarm-template.....	275
profile alarm-templateshow line-alarm-profile.....	276
profile alarm-template show port	276
profile alarm-template show virtual-noise.....	276
profile alarm-template show dpbopsd	276
profile alarm-template show rfi-bands.....	276
profile alarm-template show psd.....	277
profile alarm-template new.....	277
profile alarm-template del	277
profile alarm-template set line-alarm-profile	277
profile alarm-template set chan-alarm-profile.....	278
profile line-alarm-profile	278
profile line-alarm-profile show sprofile.....	278
profile line-alarm-profile show line-profile	280
profile line-alarm-profile show chan-profile	280
profile line-alarm-profile show alarm-template.....	280
profile line-alarm-profile show line-alarm-profile	280
profile line-alarm-profile show port.....	280
profile line-alarm-profile show virtual-noise	281
profile line-alarm-profile show dpbopsd	281
profile line-alarm-profile show rfi-bands	281
profile line-alarm-profile show psd	281
profile line-alarm-profile new	282
profile line-alarm-profile del.....	282
profile line-alarm-profile set xtucFecs	282
profile line-alarm-profile set xtucEs	282
profile line-alarm-profile set xtucSes	283
profile line-alarm-profile set xtucLoss.....	283
profile line-alarm-profile set xtucUas.....	283
profile line-alarm-profile set xturFecs.....	283
profile line-alarm-profile set xturEs	284
profile line-alarm-profile set xtucSes.....	284

profile line-alarm-profile set xturLoss	284
profile line-alarm-profile set xturUas	284
profile line-alarm-profile set fullInt	285
profile line-alarm-profile set shrtInt	285
profile chan-alarm-profile show	285
profile chan-alarm-profile show sprofile	285
profile chan-alarm-profile show line-template	287
profile chan-alarm-profile show line-profile	287
profile chan-alarm-profile show chan-profile.....	287
profile chan-alarm-profile show alarm-template.....	288
profile chan-alarm-profile show line-alarm-profile	288
profile chan-alarm-profile show port	288
profile chan-alarm-profile show virtual-noise.....	288
profile chan-alarm-profile show dpbopsd	288
profile chan-alarm-profile show rfi-bands.....	289
profile chan-alarm-profile show psd	289
profile chan-alarm-profile new	289
profile chan-alarm-profile del.....	289
profile chan-alarm-profile set cvThresXtuc.....	290
profile chan-alarm-profile set correctedThresXtuc	290
profile chan-alarm-profile set cvThresXtur	290
profile chan-alarm-profile set correctedThresXtur	290
profile pre-define.....	291
profile pre-define.....	291
profile pre-define show.....	291
profile pre-define show sprofile	291
profile pre-define show line-template	293
profile pre-define show line-profile	293
profile pre-define show chan-profile.....	293
profile pre-define show alarm-template.....	293
profile pre-define show line-alarm-profile	294
profile pre-define show port.....	294
profile pre-define show virtual-noise	294
profile pre-define show dpbopsd	294
profile pre-define show rfi-bands	294
profile pre-define show psd	295

profile pre-define vn-new	295
profile pre-define vn-del	295
profile pre-define dep-new	295
profile pre-define dep-del	296
profile pre-define rfi-new	296
profile pre-define rfi-del	296
profile pre-define vn-set-ds	296
profile pre-define vn-set-us	297
profile pre-define dep-set	297
profile pre-define rfi-set	297
profile port	298
profile port show	298
profile port show sprofile	298
profile port show line-template	299
profile port show line-profile	300
profile port show chan-profile	300
profile port show alarm-template	300
profile port show line-alarm-profile	300
profile port show port	300
profile port show virtual-noise	301
profile port show dpbopsd	301
profile port show rfi-bands	301
profile port show psd	301
profile port initprofile	302
profile port set	302
profile port set line-template	302
profile port set alarm-template	302
profile chan-profile	303
profile chan-profile new	303
profile chan-profile del	303
profile chan-profile set	303
profile chan-profile set minDataRateDsCh1	304
profile chan-profile set minDataRateUsCh1	304
profile chan-profile set maxDataRateDsCh1	304
profile chan-profile set maxDataRateUsCh1	304
profile chan-profile set maxDelayDsCh1	305

profile chan-profile set maxDelayUsCh1	305
profile chan-profile set minInpDsCh1	305
profile chan-profile set minInpUsCh1	305
profile chan-profile set minInp8DsCh1	306
profile chan-profile set minInp8UsCh1	306
7. LAYER 2 OPERATION.....	307
7.1 Address Table	307
7.2 Learning	307
7.3 Forwarding & Filtering.....	307
7.4 Store-and-Forward	307
7.5 Auto-Negotiation	308
8. TROUBLE SHOOTING.....	309
APPENDIX A—RJ-45 PIN ASSIGNMENT	311
A.1 DSLAM's RJ-45 Pin Assignments.....	311
A.2 10/100Mbps, 10/100Base-TX.....	311
A.3 RJ-21 Connector pin out for VDL-2420MR Series	313
A.4 RJ-21 / Telco 50 Cable pin out	314

1. Introduction

The PLANET VDL-2420MR, VDL-2420MR48, are multiple VDSL2 ports IP DSLAM with Gigabit TP/SFP fiber optical combo connective ability and robust layer 2 features; the description of these models as below:

VDL-2420MR : 24-Port VDSL2 IP DSLAM / AC Power

VDL-2420MR48 : 24-Port VDSL2 IP DSLAM / DC Power



VDL-2420MR / VDL-2420MR48

Terms of “**IP DSLAM**” means the device mentioned titled in the cover page of this User’s manual, i.e., VDL-2420MR and VDL-2420MR48.

1.1 Package Contents

Open the box of the IP DSLAM and carefully unpack it. The box should contain the following items:

Check the contents of your package for following parts:

<input checked="" type="checkbox"/> The IP DSLAM	x1
<input checked="" type="checkbox"/> User’s Manual CD	x1
<input checked="" type="checkbox"/> Quick Installation Guide	x1
<input checked="" type="checkbox"/> 19” Rack mount Accessory Kit	x1
<input checked="" type="checkbox"/> Power Cord	x1
<input checked="" type="checkbox"/> Rubber Feet	x4
<input checked="" type="checkbox"/> RS-232 DB9 female Console Cable	x1
<input checked="" type="checkbox"/> 2 meter Telco-50 Cable	X2

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.



VDL-2420MR or VDL-2420MR48 comes with one power system by default. The power slot 2 is vacant slot and can be installed with VC-RPS200 or VC-RPS48, please consult your local dealer for the order information.

1.2 Product Description

Over view

Perfectly designed for FTTx last mile applications

The PLANET VDL-24240MR series is a telecom-level high performance **VDSL2 IP-DSLAM** (Digital Subscriber Line Access Multiplexer) with **24-Port VDSL2**, **2-Port Gigabit TP / SFP** combo interfaces, Hot-Swappable **AC/DC Redundant Power System** and robust Layer 2+ switching features. The VDL-2420MR series is fully compliant with the ITU-T G.993.2 standard and supports VDSL2 30a profiles to offer maximum download and upload line rate up to **100/100Mbps** on the existing twisted pair lines. The VDL-2420MR helps service providers to easily provide high bandwidth demanded triple-play services such as IPTV, HDTV, Video Phone and Internet Gaming at the same copper line and uplink to the core / metro Ethernet network through the two Gigabit fiber optical interfaces. It is an ideal CO solution for **FTTx last mile** applications of broadband access by ISPs, Telecoms and campuses.

Comprehensive and Advanced VDSL2 Configuration

For the bandwidth and distance of broadband access, the VDL-2420MR VDSL2 IP-DSLAM supports multiple selective VDSL2 profiles (8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a) and 997/998 Band plan to each subscriber line. To help the ISPs provide always on internet access service in different physical line installation environments, the VDL-2420MR supports configurable **DPBO** (Downstream Power Back-Off) and **UPBO** (Upstream Power Back-Off) to adjust the downstream / upstream transmit power levels for service provider to reduce the interference by nearby wires. Furthermore, it can be configured on a per-link basis for transmission mode, rate limitation and SNR (signal-to-noise) margin. These advanced VDSL2 functionalities help service providers to adjust the line performance to ensure the VDSL2 service not be impacted by other xDSL services in the same binder group and building a stable and reliable IP DSLAM solution.

Extremely Reliable Design to Ensure Continuous Operation

The VDL-2420MR Series supports the optional hot-swappable **Redundant Power System (RPS)** to ensure continuous operation. The VDL-2420MR equips with one 100~240V AC power supply unit and the VDL-2420MR48 equips with one DC -48V power supply unit on their standard package. To enhance the reliability, both the VDL-2420MR and VDL-2420MR48 provide one spare power supply unit slot for optional 100~240V AC or DC -48V redundant power supply installation. The continuous power systems are specifically designed to handle high tech facilities requiring the highest power integrity available. Also, the -48V DC power supply implemented makes the VDL-2420MR Series VDSL2 Switch as a telecom level device that can be located at the electronic room.



VDL-2420MR – One 100~240V AC



VDL-2420MR48 – One -48VDC

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

The section explains the functions of the IP DSLAM and how to physically install the IP DSLAM.

Section 3, DSLAM MANAGEMENT

The section contains the information about the software function of the IP DSLAM.

Section 4, WEB CONFIGURATION

The section explains how to manage the IP DSLAM by Web interface.

Section 5, CONSOLE MANAGEMENT

The section describes how to use the Console management interface.

Section 6, COMMAND LINE INTERFACE

The section explains how to manage the IP DSLAM by Command Line interface.

Section 7, DSLAM OPERATION

The chapter explains how to does the IP DSLAM operation of the IP DSLAM.

Section 8, TROUBLESHOOTING

The chapter explains how to trouble shooting of the IP DSLAM.

Appendix A

The section contains cable information of the IP DSLAM.

1.4 Product Features

➤ VDSL Interface

- 24 Full-Duplex VDSL links via RJ-21(Telco-50) connector
- 24 corresponding POTS lines via RJ-21(Telco-50) connector
- Built-in POTS splitter for each VDSL port
- Link to VC-231 / VC-234 / VC-230N CPE Bridge
- Auto-speed function for VDSL2 link (by distance and cable quality)

➤ Ethernet Interface

- 2 10/100/1000Mbps TP and SFP shared combo interfaces
- Auto-MDI/MDI-X detection on Gigabit RJ-45 port

➤ VDSL2 Features

- Cost-effective VDSL2 link and central management solution
- Compliant with VDSL2 standard:
 - ITU-T G.993.2
 - ITU-T G-994.1
 - ITU-T G.997.1
- ITU-T G.993.2, 8a / 8b / 8c / 8d / 12a / 12b / 17a / 30a Profiles
- Configurable Line Template and Alarm Template
- Configurable UPBO / DPBO / US0 Allow / Virtual Noise PSD
- Configurable Bitswap / G.hs carrier set / RFI Band
- Manual / Ralnit / Dynamic Rate Adaption
- DMT (Discrete Multi-Tone) line coding VDSL
- Up to 100/100Mbps symmetric data rate
- Selectable target data rate and target SNR margin
- Built-in surge protection to against surge damage from high energy spike
- Voice and data communication can be shared on the existing telephone wire simultaneously
- Supports Downstream / Upstream rate control on each port

➤ Layer 2 Features

- High performance of Store-and-Forward architecture, runt/CRC filtering eliminate erroneous packets to optimize the network bandwidth
- Broadcast / Multicast / Unicast storm control
- Support VLAN
 - IEEE 802.1Q Tag-based VLAN
 - Port-based VLAN
 - Q-in-Q tunneling (VLAN Stacking)
 - GVRP for dynamic VLAN management
 - Private VLAN Edge (PVE / Protected port)
- Link Aggregation
 - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
 - Cisco ether-channel (Static Trunk)
- Spanning Tree Protocol

- STP, IEEE 802.1D (Classic Spanning Tree Protocol)
- MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, Spanning Tree by VLAN)
- Port Mirroring to monitor the incoming or outgoing traffic on a particular port
- PPPoE packet pass-through
- VPN pass-through

➤ **Quality of Service**

- 4 priority queues on all switch ports
- Traffic classification:
 - IEEE 802.1p CoS
 - IP TOS / DSCP to 802.1p priority mapping
 - Port-Based priority
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Voice QoS by application source / destination protocol no.

➤ **Multicast**

- Supports IGMP Snooping v1 and v2
- IGMP Snooping v2 fast leave
- Querier mode support

➤ **Security**

- IEEE 802.1x Port-based network access control protocol
- RADIUS users access authentication
- L3 / L4 Access Control List (ACL)
- MAC Filtering and Source IP-MAC / Port-Binding
- Port Security for Source MAC address entries filtering

➤ **Management**

- Switch Management Interface
 - Telnet Command Line Interface
 - Web switch management
 - SNMP v1, v2c, v3 switch management
 - SSL switch management
- DHCP client for IP address assignment
- DHCP Option82 and DHCP Relay
- SNTP (Simple Network Time Protocol)
- Built-in Trivial File Transfer Protocol (TFTP) client
- Firmware upgrade via TFTP or HTTP
- Configuration upload/download via TFTP or HTTP
- Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events)
- SNMP trap for interface Link Up and Link Down notification
- Logging to remote syslog server
- Link Layer Discovery Protocol (LLDP) for easy network management
- Supports Ping function
- Reset button for system management
- 1 RS-232 male DB9 console interface for Switch basic management and setup
- User privilege control – admin, operator, viewer

➤ **Redundant Power System**

- 100~240V AC / 48V DC Dual power redundant (Optional)
- Active-active redundant power failure protection
- Backup of catastrophic power failure on one supply

1.5 Product Specification

Product		VDL-2420MR	VDL-2420MR48
Hardware Specification			
VDSL Interface	24-Port VDSL2 Line via 1 RJ-21 (Telco-50) connector		
	24-Port POTS/Telephone via 1 RJ-21 (Telco-50) connectors		
1000Mbps Copper Ports	2 10/100/1000Mbps RJ-45 Auto-negotiation, Auto MDI/MDI-X		
SFP/mini-GBIC Slots	2 1000Base-SX/LX/BX, shared with Port-25~Port-26		
Console	1 x RS-232 Serial Port (DB9, 57600, N, 8, 1)		
Surge Protect	3KV		
Switch Architecture	Store-and-Forward		
Switch Fabric	8.8Gbps / non-blocking		
Switch Throughput	6.547Mpps @64Bytes		
Address Table	8K entries		
Share Data Buffer	512Kbytes		
Maximum Frame Size	9K Bytes		
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex		
LED	System: Power, SYS Status Alert: FAN 1, FAN 2, Power 1, Power 2 VDSL: VDSL Link/Sync. Gigabit Port: 1000 Link/Active, 100 Link/Active		
Reset Button	< 5 sec: System reboot > 10 sec: Factory Default		
Dimension (W x D x H)	440 x 300 x 44 mm, 2U height		
Weight	6.4kg		
Power Requirement	AC Input	100~240V AC, 50-60 Hz	Optional AC Power module
	DC Input	Optional DC Power module	-48V DC; Range: 30V~60V
Power Consumption / Dissipation	130Watts maximum / 404 BTU/hr maximum		
Standard Accessory	<ul style="list-style-type: none"> - 2-Meter Telco-50 Cable x 2 - FAN Module x 1 - 19" rack mount kit 		
VDSL2			
VDSL2 Standard	Comply with ITU-T G.993.2. Supports provisioning the VDSL optional band (25K to 138K Hz) usage ITU-T G.994.1: Handshake procedure of each DMT xDSL circuit ITU-T G.997.2: Physical layer management of each DMT xDSL circuit		
Encoding	VDSL-DMT		
VDSL2 Template	Configurable Line Template Configurable Alarm Template		
Line Interface			

VDSL2 Profile	Selectable spectrum profile of - 8a / 8b / 8c / 8d / 12a / 12b / 17a / 30a
Band Plan	Selectable band plan for each VDSL line on a per port basis Band plan A: - Profile 998, Annex A of G.993.1; Optimized for symmetric services Band plan B: - Profile 997, Annex B of G.993.1 ; Optimized for asymmetric services
Rate Adaptation	Manual Rate Dynamics
Power Back-Off	Downstream Power Back-Off (DPBO) PSD Upstream Power Back-Off (UPBO) PSD
VDSL2 Features	Selectable rate limit control Selectable target SNR (signal to Noise Ratio) mode POTS voices pass through
POTS Splitter	Compliant with ETSI TS 101 952-1-1 option A for European The splitter is passive element. Even the system is loss of power, the POTS service is still OK
Layer 2 Function	
Management Interface	Console, Telnet, Web Browser, SSL, SNMPv1 / v2c / v3
Gigabit Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable
Gigabit Port Status	Display each port's speed duplex mode, link status and Flow control status. Auto negotiation status, trunk status.
Port Mirroring	TX / RX / Both 1 to 1 monitor
Bandwidth Control	Ingress / Egress rate limit control Gigabit Port: <ul style="list-style-type: none"> Allow to configure per 128Kbps VDSL2 Port: <ul style="list-style-type: none"> Allow to configure per 4kbps
VLAN	IEEE 802.1Q Tag-based VLAN, up to 256 VLAN groups, out of 4041 VLAN IDs Port-based VLAN, up to 26 VLAN groups GVRP, up to 128 dynamic VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE / Protected port) with two protected port groups Support Asymmetric VLAN membership configuration
Spanning Tree Protocol	IEEE 802.1D Spanning Tree IEEE 802.1s Multiple Spanning Tree Up to 16 MST instances (0~15)
Link Aggregation	Static Port Trunk IEEE 802.3ad LACP (Link Aggregation Control Protocol) Supports 13 groups of 8-Port trunk support
QoS	4 priority queue Traffic classification based on

	<ul style="list-style-type: none"> - Port priority - 802.1p priority - DSCP/TOS field in IP Packet <p>VoIP QoS by application protocol no.</p>																																																
IGMP Snooping	IGMP (v1/v2) Snooping, up to 256 multicast Groups																																																
Access Control List	IP-based Layer 3 / Layer 4 ACL Up to 220 ACL rule entries																																																
Security	<p>Port Security – supports per port MAC limit up to 64 entries</p> <p>Static MAC and MAC Filter – up to 256 MAC address entries</p> <p>Source IP / Source MAC Address and Port binding</p> <p>IEEE 802.1X Port-Based Network Access Control – supporting authentication types:</p> <ul style="list-style-type: none"> - EAP-MD5 / EAP-TLS / EAP-PEAP 																																																
SNMP MIBs	<p>RFC-1213 MIB-II</p> <p>RFC-2863 Interface MIB</p> <p>RFC-2665 EtherLike MIB</p> <p>RFC-1493 Bridge MIB</p> <p>RFC-2819 RMON MIB (Group 1, 2, 3,9)</p> <p>RFC-2737 Entity MIB</p> <p>RFC 5650 VDSL2 MIB</p>																																																
Standards Conformance																																																	
Regulation Compliance	FCC Part 15 Class A, CE																																																
Standards Compliance	<table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 50%;">IEEE 802.3</td><td>10Base-T</td></tr> <tr><td>IEEE 802.3u</td><td>100Base-TX</td></tr> <tr><td>IEEE 802.3z</td><td>1000Base- SX / LX</td></tr> <tr><td>IEEE 802.3ab</td><td>1000Base-T</td></tr> <tr><td>IEEE 802.3x</td><td>Flow Control and Back pressure</td></tr> <tr><td>IEEE 802.3ad</td><td>Link Aggregation Control Protocol (LACP)</td></tr> <tr><td>IEEE 802.1D</td><td>Spanning tree protocol</td></tr> <tr><td>IEEE 802.1s</td><td>Multiple Spanning tree protocol</td></tr> <tr><td>IEEE 802.1p</td><td>Class of service</td></tr> <tr><td>IEEE 802.1Q</td><td>VLAN tagging</td></tr> <tr><td>IEEE 802.1x</td><td>Port-based authentication network control</td></tr> <tr><td>ITU-T</td><td>G.997.1</td></tr> <tr><td></td><td>G.993.2 VDSL2 (Profile 30a Support), Annex A</td></tr> <tr><td>RFC 768</td><td>UDP</td></tr> <tr><td>RFC 783</td><td>TFTP</td></tr> <tr><td>RFC 791</td><td>IP</td></tr> <tr><td>RFC 792</td><td>ICMP</td></tr> <tr><td>RFC 854</td><td>Telnet</td></tr> <tr><td>RFC 2068</td><td>HTTP</td></tr> <tr><td>RFC 1112</td><td>IGMP version 1</td></tr> <tr><td>RFC 1157</td><td>SNMPv1</td></tr> <tr><td>RFC 1902</td><td>SNMPv2</td></tr> <tr><td>RFC 2236</td><td>IGMP version 2</td></tr> <tr><td>RFC 5424</td><td>Syslog</td></tr> </table>	IEEE 802.3	10Base-T	IEEE 802.3u	100Base-TX	IEEE 802.3z	1000Base- SX / LX	IEEE 802.3ab	1000Base-T	IEEE 802.3x	Flow Control and Back pressure	IEEE 802.3ad	Link Aggregation Control Protocol (LACP)	IEEE 802.1D	Spanning tree protocol	IEEE 802.1s	Multiple Spanning tree protocol	IEEE 802.1p	Class of service	IEEE 802.1Q	VLAN tagging	IEEE 802.1x	Port-based authentication network control	ITU-T	G.997.1		G.993.2 VDSL2 (Profile 30a Support), Annex A	RFC 768	UDP	RFC 783	TFTP	RFC 791	IP	RFC 792	ICMP	RFC 854	Telnet	RFC 2068	HTTP	RFC 1112	IGMP version 1	RFC 1157	SNMPv1	RFC 1902	SNMPv2	RFC 2236	IGMP version 2	RFC 5424	Syslog
IEEE 802.3	10Base-T																																																
IEEE 802.3u	100Base-TX																																																
IEEE 802.3z	1000Base- SX / LX																																																
IEEE 802.3ab	1000Base-T																																																
IEEE 802.3x	Flow Control and Back pressure																																																
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)																																																
IEEE 802.1D	Spanning tree protocol																																																
IEEE 802.1s	Multiple Spanning tree protocol																																																
IEEE 802.1p	Class of service																																																
IEEE 802.1Q	VLAN tagging																																																
IEEE 802.1x	Port-based authentication network control																																																
ITU-T	G.997.1																																																
	G.993.2 VDSL2 (Profile 30a Support), Annex A																																																
RFC 768	UDP																																																
RFC 783	TFTP																																																
RFC 791	IP																																																
RFC 792	ICMP																																																
RFC 854	Telnet																																																
RFC 2068	HTTP																																																
RFC 1112	IGMP version 1																																																
RFC 1157	SNMPv1																																																
RFC 1902	SNMPv2																																																
RFC 2236	IGMP version 2																																																
RFC 5424	Syslog																																																

Cables	<ul style="list-style-type: none"> • VDSL2: twisted-pair telephone wires (AWG24 or better) up to 1.4km • 10/100Base-TX: 2-Pair UTP Cat.5, up to 100m (328ft) • 1000Base-T: 4-pair UTP Cat.5E, up to 100m • 1000Base-SX: 50/125µm and 62.5/125µm fiber-optic cable, up to 550m • 1000Base-LX: 9/125µm fiber optic cable, up to 10km 50/125µm and 62.5/125µm fiber-optic cable, up to 550m
Environment	
Temperature	0~50 Degree C
Humidity	5~95% (non-condensing)

VDL-2420MR or VDL-2420MR48 only equipped with one power system, the optional power system can be ordered by request with model no. VC-RPS200 for AC power source and VC-RPS48 for DC power source.

* VDSL2 CPE: PLANET VC-231

2. INSTALLATION

This section describes the hardware features and installation of the IP DSLAM on the desktop or rack mount. For easier management and control of the IP DSLAM, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the IP DSLAM, please read this chapter completely.

2.1 Hardware Description

2.1.1 DSLAM Front Panel

The unit front panel provides a simple interface monitoring the IP DSLAM. [Figure 2-1-1](#) shows the front panel of the IP DSLAM.

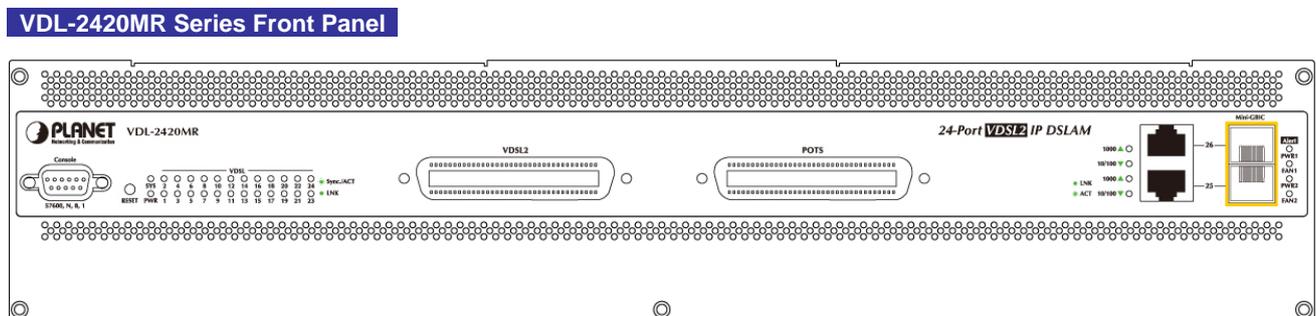


Figure 2-1-1: VDL-2420MR Series front panel

■ Console Port

The console port is a DB9, RS-232 male serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information includes IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

■ VDSL2 and POTS interface

There are 24 VDSL2 ports and 24 POTS ports with 2 Telco-50 / RJ-21 type connectors on the front panel of VDL-2420MR series. Each port is built-in POTS splitter that helps the voice of telephone and data of network applications transmitting at the same wire without interrupted.

The VDSL2 supports auto detection transmission rate that operate in different band allocation and result in different upstream and downstream bandwidth. And Due to different telephone line quality, cross talk or extension distance may affect actual achievable speed; you can configure individual port in built-in management interface for optimized connectivity.



1. The payload rate is about 9% less than the line rate due to framing overhead.
2. AWG 26 (0.4mm) cable can also be used but the distance is 20% to 40% shorter than above table.
3. Each terminated bridge tap can reduce the VDSL link distance by 90m. The quality of the cable, the size of the cable bundles, and the cross talk within the bundle, can also affect other overall reach.

■ Gigabit TP Interface

VDL-2420MR Series: Port-25 and Port-26

10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

■ Gigabit SFP Slots

VDL-2420MR Series: Port-25 and Port-26

1000Base-SX/LX mini-GBIC slot, SFP (Small Form-Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber), up to 10/30/50/70/120 kilometers (Single-mode fiber).

■ Reset button

At the left of front panel, the reset button is designed for reboot the IP DSLAM without turn off and on the power. The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
About 1~5 second	Reboot the IP DSLAM
Until the SYS LED lit off	Reset the IP DSLAM to Factory Default configuration. The IP DSLAM will then reboot and load the default settings as below: <ul style="list-style-type: none"> ◦ Default Password: admin ◦ Default IP address: 192.168.0.100 ◦ Subnet mask: 255.255.255.0 ◦ Default Gateway: 192.168.0.254

2.1.2 LED Indications

The front panel LEDs indicates instant status of port links, data activity and system power; helps monitor and troubleshoot when needed.

VDL-2420MR Series LED indication

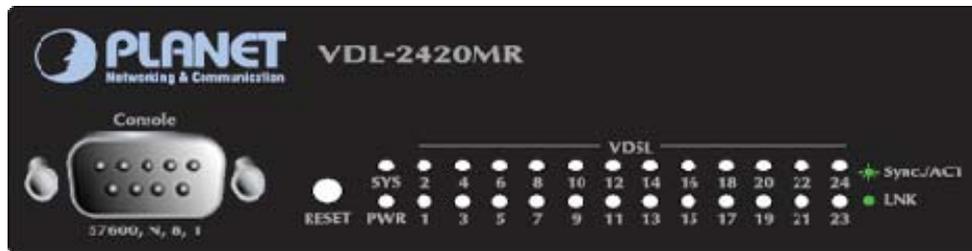


Figure 2-1-2: VDL-2420MR Series System and Port LED panel

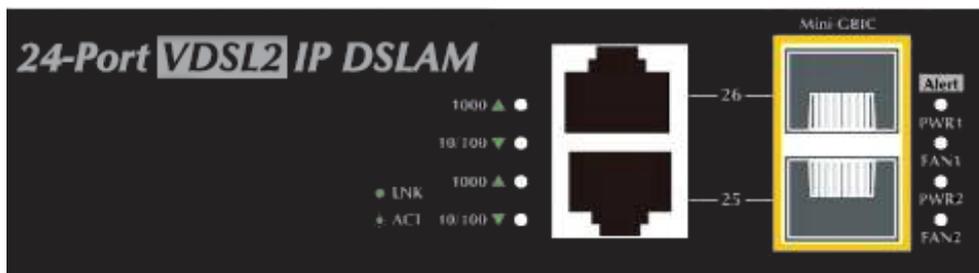


Figure 2-1-3: VDL-2420MR Series Power and fan LED panel

■ System

LED	Color	Function	
PWR	Green	On:	Indicate that the IP DSLAM is powered on .
		Off:	Indicate that the IP DSLAM is powered off .
SYS	Orange	Lit:	Lights to indicate the system is working.
		Blink:	Indicate that the system is in OS boot procedure or reset to default.
PWR1	Orange	On:	Indicate that power1 is inserted and failed to work.
FAN1	Orange	On:	Indicate that fan1 is failed to work.
PWR2	Orange	On:	Indicate that power2 is inserted and failed to work.
FAN2	Orange	On:	Indicate that fan2 is failed to work.

■ Per VDSL Interface (Port-1 to Port-24)

LED	Color	Function	
VDSL LNK/Sync	Green	On:	Indicate that the VDSL link is established.
		Slow Blink:	Indicate that the VDSL is at training status with remote CPE
		Quick Blink:	Indicate that the DATA link is actively sending or receiving data over that VDSL port
		Off:	Indicate that the VDSL is link down

■ 10/100/1000Base-T Copper / 1000Base-SX/LX SFP Interface (Port-25 and Port-26)

LED	Color	Function	
1000 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 1000Mbps
		Blink:	To indicate that the IP DSLAM is actively sending or receiving data over that port.
		Off:	If 10/100 LNK/ACT LED is light, it indicates that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED is Off, it indicates that the port is link down
10/100 LNK/ACT	Green	On:	To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink:	To indicate that the IP DSLAM is actively sending or receiving data over that port.
		Off:	If 1000 LNK/ACT LED is light, indicates that the port is operating at 1000Mbps If 1000 LNK/ACT LED is Off, it indicates that the port is link down



The 2 Gigabit TP/SFP combo ports are shared with Port25/26 of VDL-2420MR Series. Either of them can operate at the same time.

2.1.3 IP DSLAM Rear Panel

The VDL-2420MR equip with one 100~240V AC power supply unit and VDL-2420MR48 equip with one DC -48V power supply unit on its standard package, both VDL-2420MR and VDL-2420MR48 provide one spare power supply unit slot for option redundant power supply installation. A redundant power supply is also provided to enhance the reliability with options of either 100~240V AC power supply unit or DC -48V power supply unit.

VDL-2420MR Rear Panel

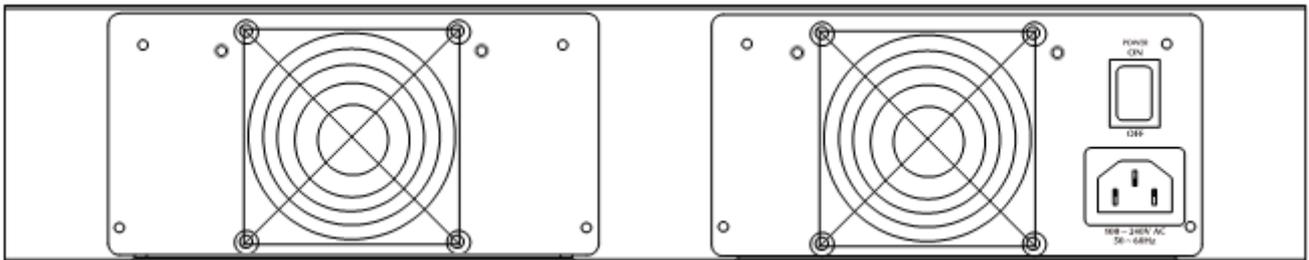


Figure 2-1-4: VDL-2420MR rear panel with AC power module

VDL-2420MR48 Rear Panel

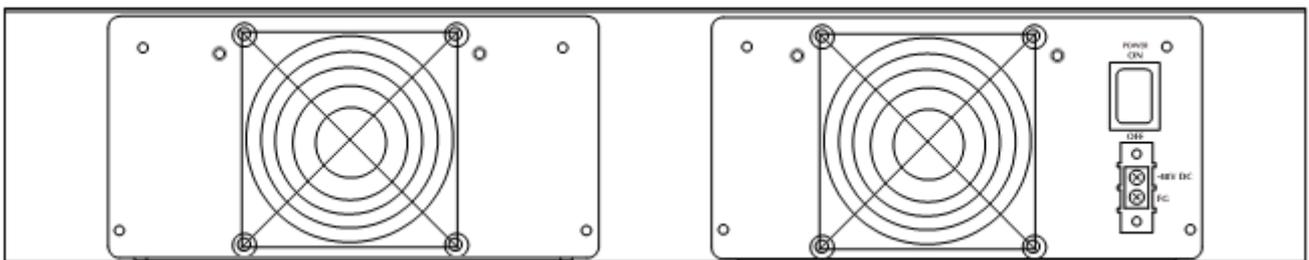


Figure 2-1-5: VDL-2420MR48 rear panel with DC power module

Install and remove the power supply unit

To install a power supply unit to VDL-2420MR series, please fasten the hand screw clockwise and slide in the power supply unit to the Managed Media Converter Chassis.

To remove a power supply unit out the VDL-2420MR series, please loose the hand screw counter clockwise and pull out the power supply unit from the VDL-2420MR series.



Figure 2-1-6: Install and remove the power supply unit of VDL-2420MR series

Power Notice:

-
1. The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.
 2. In some area, installing a surge suppression device may also help to protect your The IP DSLAM from being damaged by unregulated surge or current to the IP DSLAM or the power adapter.
-

2.2 Install the IP DSLAM

This section describes how to install the IP DSLAM and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.2.1 Rack Mounting

To install the IP DSLAM in a 19-inch standard rack, please follow the instructions described below.

Step1: Place the IP DSLAM on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the IP DSLAM with supplied screws attached to the package.

Figure 2-2-1 shows how to attach brackets to one side of the IP DSLAM.

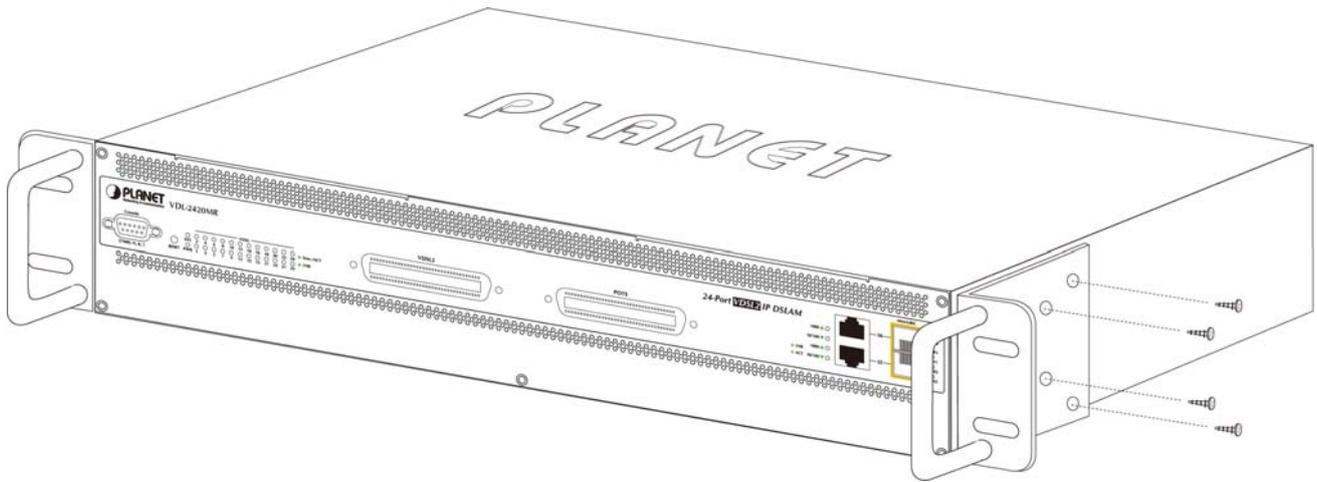


Figure 2-2-1 Attach brackets to VDL-2420MR series



You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the IP DSLAM, use suitable screws to securely attach the brackets to the rack, as shown in [Figure 2-2-2](#).

2.2.2 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the IP DSLAM. As the [Figure 2-2-3](#) appears.



Figure 2-2-3: Plug-in the SFP transceiver

Approved PLANET SFP Transceivers

PLANET IP DSLAM supports both single mode and multi mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

1000Base-SX/LX SFP transceiver:

- **MGB-SX** SFP (1000BASE-SX SFP transceiver – Multi mode / 220m)
- **MGB-LX** SFP (1000BASE-LX SFP transceiver - Single Mode / 10km)
- **MGB-L30** SFP (1000Base-LX SFP transceiver – Single Mode / 30Km)
- **MGB-L50** SFP (1000Base-LX SFP transceiver - Single Mode / 50Km)



It recommends using PLANET SFPs on the IP DSLAM. If you insert a SFP transceiver that is not supported, the IP DSLAM will not recognize it.

Before connect to the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.

2. Check the fiber-optic cable type match the SFP transceiver model.
 - To connect to **1000Base-SX** SFP transceiver, use the **multi-mode** fiber cable- with one side must be male duplex LC connector type.
 - To connect to **1000Base-LX** SFP transceiver, use the **single-mode** fiber cable-with one side must be male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the IP DSLAM. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to “1000 Force” is needed.

Remove the transceiver module

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the IP DSLAM/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB module to horizontal.
4. Pull out the module gently through the handle.



Figure 2-2-4: Pull out the SFP transceiver



Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the IP DSLAM.

2.3 Wiring for VDSL2 Ports

The VDSL2 port of VDL-2420MR series uses one RJ-21 (Telco 50) connector to connect to a patch panel then link up to 24 VDSL CPEs which can be just directly connected to the remote CPEs (VC-230, VC-230N, VC-231, VC-234 or other compatible CPE) through structured or unstructured wiring, such as existing telephone lines. The link between the VDSL2 CO DSLAM port and each CPE can reach speeds of up to 100/100 Mbps under 1000 feet (300 meters) with profile 30a or 18/1 Mbps over distances of up to 5000 feet (1500 meters). You can hot swap the VDSL2 CPEs without powering down the IP DSLAM or disrupting the other DSLAM ports.

Each VDL-2420MR series had built-in **Pain Old Telephone service (POTS)** splitter to transmit both VDSL2 traffic and telephone services, such as voice or Fax, through same phone wire. The splitter routes VDSL2 data (high-frequency) and voice (low-frequency) traffic from the telephone line and **Private Branch exchange (PBX)** DSLAM or **Public Switched Telephone Network (PSTN)**.

The connection diagrams are as the following.

■ VDL-2420MR Series VDSL2 and POTS connection

For the 24-Port VDSL or 24-PORT POTS, there are 24 pairs are used for tip and ring. The top row of the Telco RJ-21 connector is tip and the bottom row is ring. [Figure 2-3-1](#) shows the pin out convention for the RJ-21 connector.

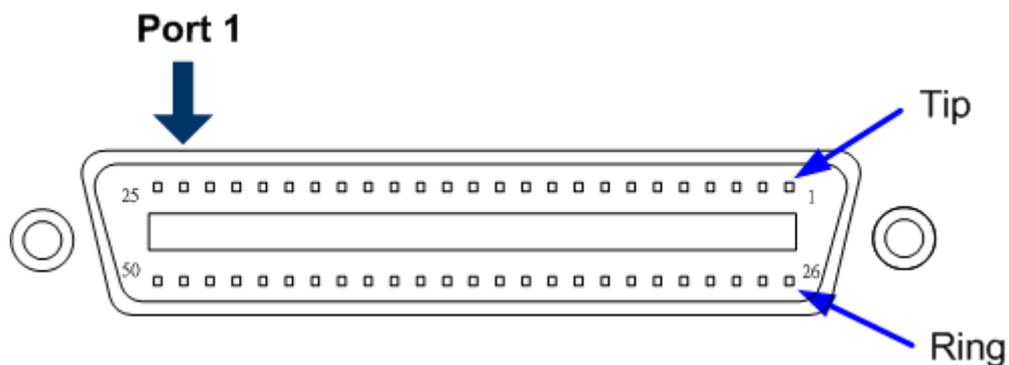


Figure 2-3-1 Pin out convention for the Telco RJ-21 connector of VDL-2420MR series



To get the pin assignment of the VDSL/POTS port numbers to the pin numbers on the RJ-21 of the VDL-2420MR series, please refer to [APPENDIX A.3](#) for more detail.

The VDSL port and POTS port of VDL-2420MR series always connects to a patch panel. The connection between the VDL-2420MR series and the patch panel is made by an RJ-21 Category 5 Telco interface connector and cable, as shown in [Figure 2-3-2](#) and [Figure 2-3-3](#).

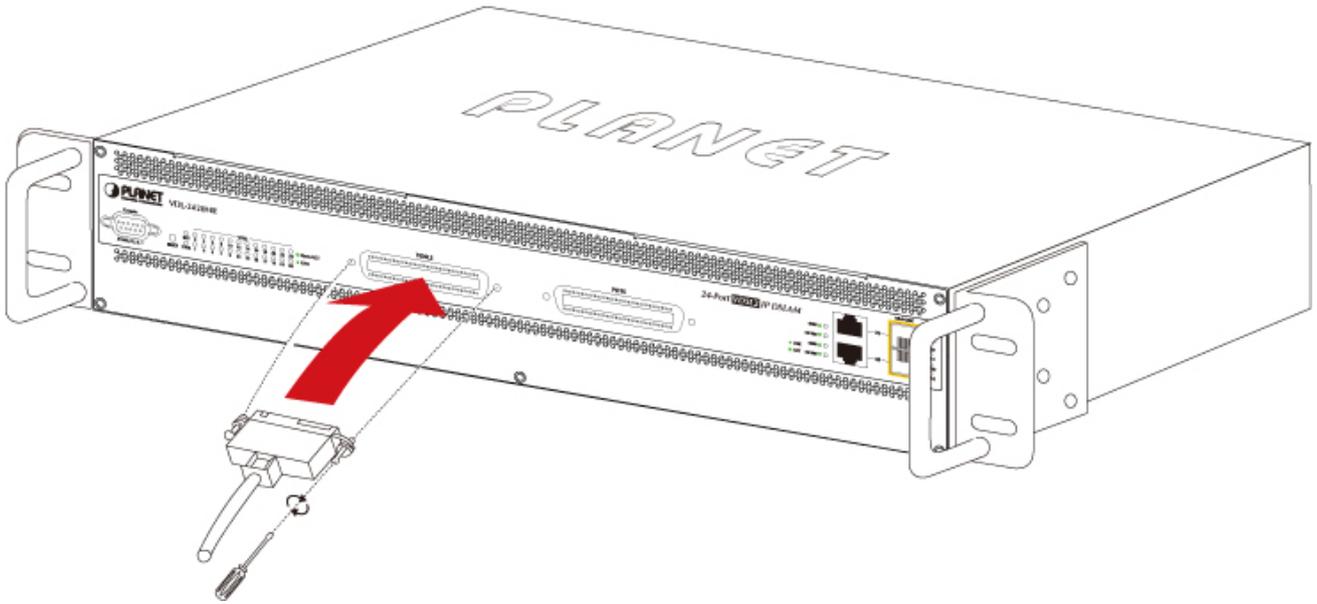


Figure 2-3-2 Telco RJ-21 connect to VDL-2420MR series

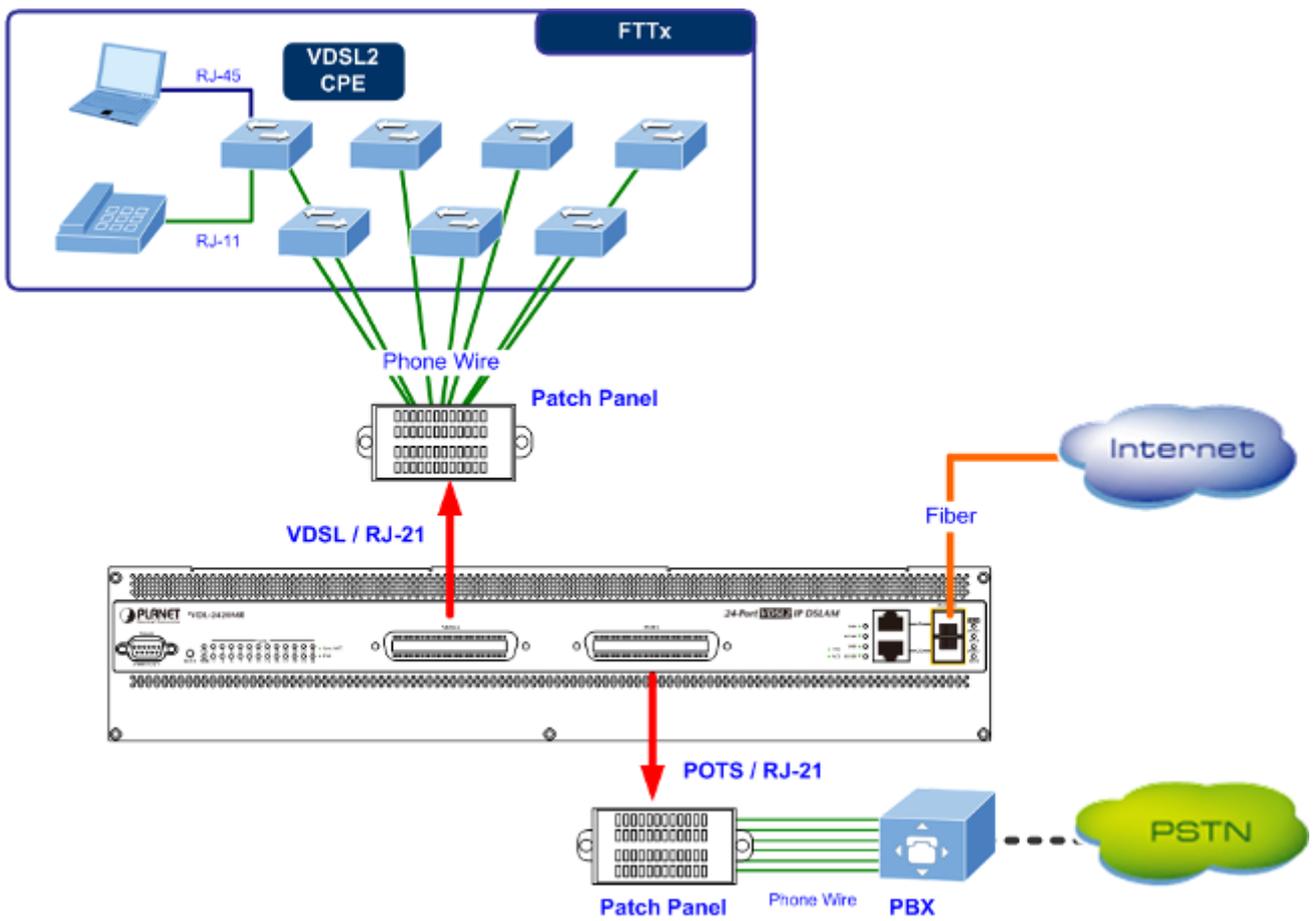


Figure 2-3-3: VDL-2420MR Series VDSL2 connection

3. DSLAM MANAGEMENT

This chapter explains the methods that you can use to configure management access to the IP DSLAM. It describes the types of management applications and the communication and management protocols that deliver data between your management device (work-station or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** of subscribers running Windows 98/ME, NT4.0, 2000/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- Ethernet Port connect
 - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- Above Workstation installed with **WEB Browser** and **JAVA runtime environment** Plug-in
- **Serial Port** connect
 - Above PC with COM Port (DB-9 / RS-232) or USB-to-RS-232 converter



It is recommended to use Internet Explore 6.0 or above to access The IP DSLAM.

3.2 Management Access Overview

The IP DSLAM gives you the flexibility to access and manage it using any or all of the following methods:

- **Web browser** interface
- **An external SNMP-based network management application**
- **An administration console**

The administration console and Web browser interface support are embedded in the IP DSLAM software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Web Browser	<ul style="list-style-type: none"> • Ideal for configuring the IP DSLAM remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing 	<ul style="list-style-type: none"> • Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	<ul style="list-style-type: none"> • Communicates with DSLAM functions at the MIB level • Based on open standards 	<ul style="list-style-type: none"> • Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)
Console	<ul style="list-style-type: none"> • No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure 	<ul style="list-style-type: none"> • Must be near DSLAM or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow

Table 3-1: Management Methods Comparison

3.3 Web Management

The IP DSLAM offers management features that allow users to manage the IP DSLAM from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the IP DSLAM, you can access the IP DSLAM's Web interface applications directly in your Web browser by entering the IP address of the IP DSLAM.

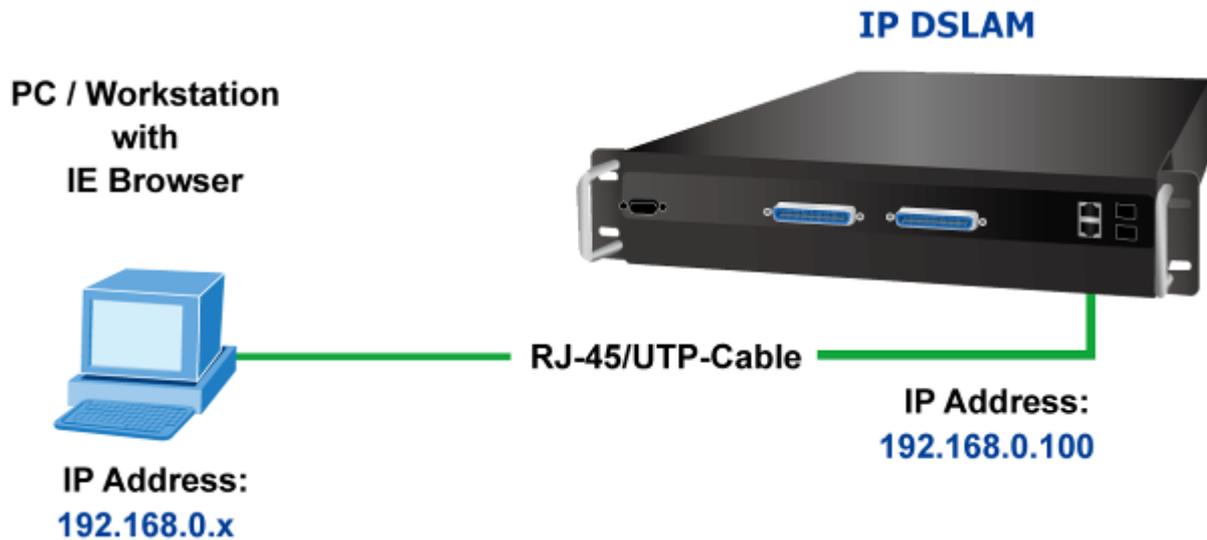


Figure 3-3-1 Web management

You can then use your Web browser to list and manage the IP DSLAM configuration parameters from one central location, just as if you were directly connected to the IP DSLAM's console port. Web Management requires either **Microsoft Internet Explorer 6.0** or later, **Safari** or **Mozilla Firefox 2.0** or later.



Figure 3-3-2 Web main screen of The IP DSLAM

3.4 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the IP DSLAM, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What'sup Gold. This management method requires the SNMP agent on the IP DSLAM and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Network management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs.

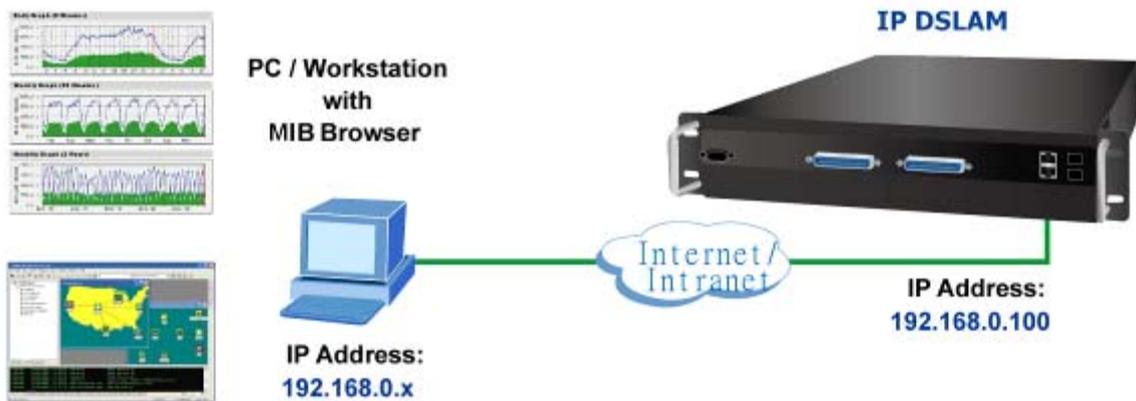


Figure 3-4-1 SNMP management

3.5 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the IP DSLAM's console (serial) port.

There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Console Management**.

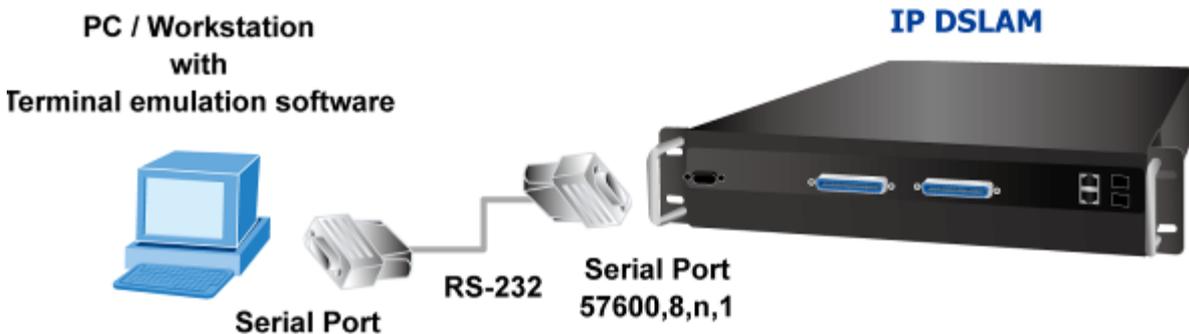


Figure 3-5-1 Console management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the IP DSLAM console (serial) port.

When using this management method, a **straight DB9 RS-232 cable** is required to connect the IP DSLAM to the PC.

After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **57600 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**



Figure 3-5-2 Terminal parameter settings

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.6 Protocols

The IP DSLAM supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.6.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as **Telnet**, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the IP DSLAM before you can establish access to it with a virtual terminal protocol.



Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.

To access the IP DSLAM through a Telnet session:

1. Be Sure of the IP DSLAM is configured with an IP address and the IP DSLAM is reachable from a PC.
2. Start the Telnet program on a PC and connect to the IP DSLAM.

The management interface is exactly the same with RS-232 console management.

3.6.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

3.6.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser). The management architecture of the IP DSLAM adheres to the IEEE open standard. This compliance assures customers that the IP DSLAM is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

4.1 About Web-based Management

The IP DSLAM offers management features that allow users to manage the IP DSLAM from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

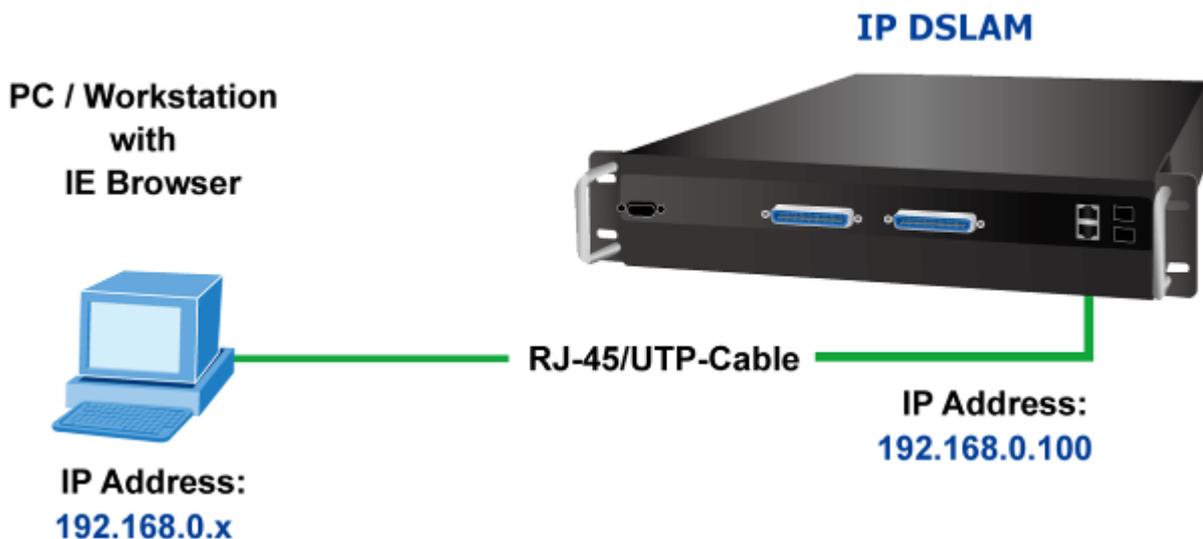


By default, IE6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The IP DSLAM can be configured through an Ethernet connection, make sure the manager PC must be set on same the IP subnet address with the IP DSLAM.

For example, the default IP address of the IP DSLAM is **192.168.0.100**, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the IP DSLAM to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.



4.1.1 Requirements

- Workstations of subscribers running Windows 98/ME, NT4.0, 2000/2003/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- Workstation installed with Ethernet NIC (Network Card).
- **Ethernet Port connect**
 - Network cables - Use standard network (UTP) cables with RJ45 connectors.
 - Above PC installed with WEB Browser and JAVA runtime environment Plug-in.



It is recommended to use Internet Explorer 6.0 or above to access VDL-2420MR series IP DSLAM.

4.1.2 Logging on the IP DSLAM

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface.
The factory-default IP Address as following:

http://192.168.0.100

2. When the following login screen appears, please enter the default user name "**admin**" with password "**admin**" (or the user name/password you have changed via console) to login the main screen of The IP DSLAM. The login screen in [Figure 4-1-1](#) appears.



Figure 4-1-1: Login screen

Default User name: **admin**

Default Password: **admin**

1. After entering the username and password, the main screen appears as [Figure 4-1-2](#).

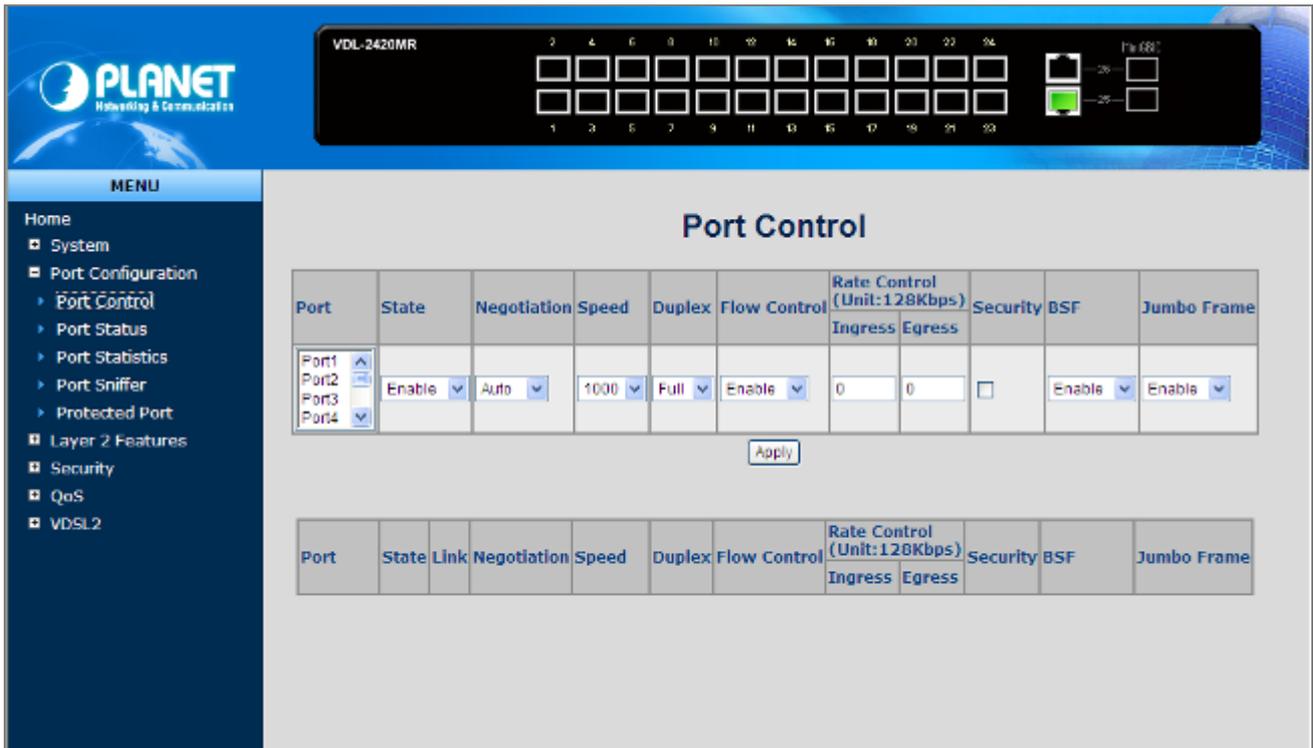


Figure 4-1-2: Web main page

2. The IP DSLAM Menu on the left of the Web page let you access all the commands and statistics the IP DSLAM provides.

Now, you can use the Web management interface to continue the IP DSLAM management or manage the IP DSLAM by Web interface. The IP DSLAM Menu on the left of the web page let you access all the commands and statistics the IP DSLAM provides.

-
1. It is recommended to use Internet Explorer 6.0 or above to access The IP DSLAM.
 2. The changed IP address take effect immediately after click on the **Apply** button, you need to use the new IP address to access the Web interface.
 3. For security reason, please change and memorize the new password after this first setup.
 4. The WEB configuration and CLI command of VDL-2420MR48 are the same with VDL-2420MR so the VDL-2420MR will be the example to describe how to configure the IP DSLAM.
-



4.1.3 Main WEB PAGE

The IP DSLAM provides a Web-based browser interface for configuring and managing it. This interface allows you to access the IP DSLAM using the Web browser of your choice. This chapter describes how to use the IP DSLAM's Web browser interface to configure and manage it.

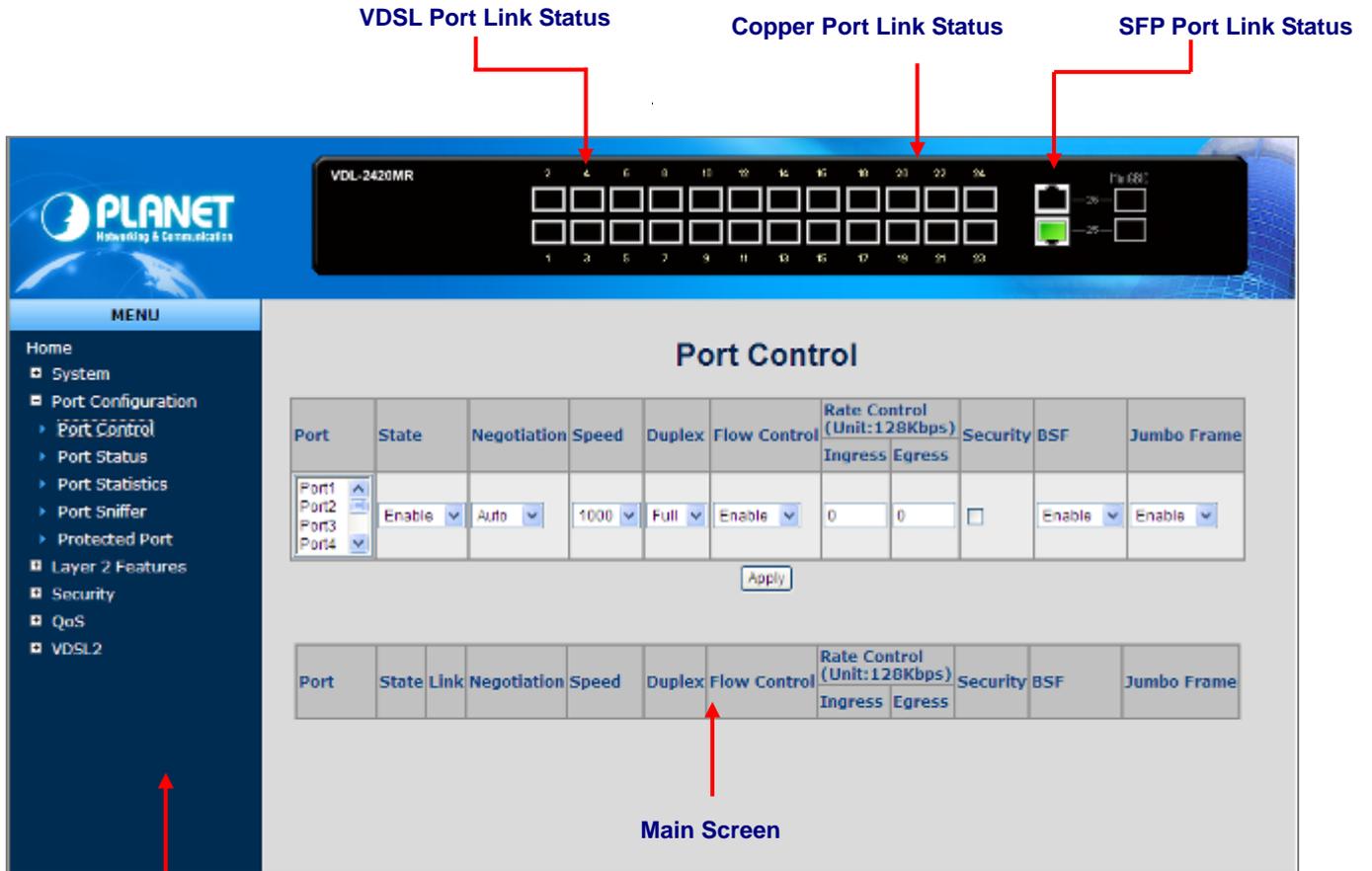


Figure 4-1-3: Main Page

Panel Display

The web agent displays an image of the IP DSLAM's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page.

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the IP DSLAM, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the IP DSLAM by select the functions those listed in the Main Function. The screen in [Figure 4-1-4](#) appears.

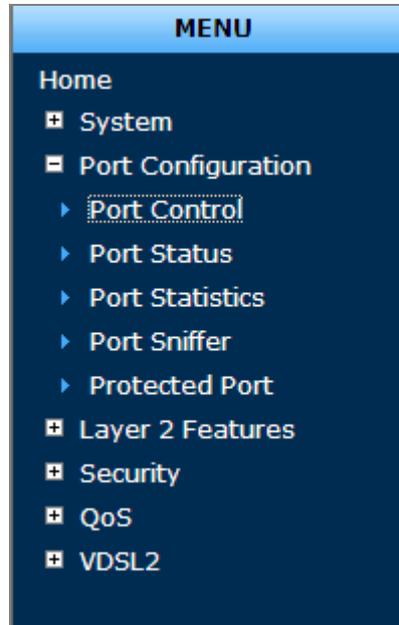


Figure 4-1-4: VDL-2420MR series Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the IP DSLAM. Under System the following topics are provided to configure and view the system information: This section has the following items:

- **System Information** Provides basic system description, including contact information.
- **IP Configuration** Sets the IP address for management access.
- **Console Information** Displays the required console settings on the IP DSLAM.
- **SNMP Configuration** Configure SNMP agent and SNMP Trap.
- **Syslog Setting** Configure logging of messages and assign IP address of remote Syslog servers.
- **Firmware Upgrade** Upgrade the firmware via TFTP server or Web Brower file transfer.
- **Configuration Backup** Save/view the IP DSLAM configuration to remote host.
Upload the IP DSLAM configuration from remote host.
- **Factory Default** Reset the configuration of the IP DSLAM.
- **System Reboot** Restarts the IP DSLAM.

4.2.1 System Information

In System information, it has two parts of setting – **Basic** and **Misc Config**. We will describe the configure detail in following.

4.2.1.1 Basic

The Basic System Info page provides information for the current device information. Basic System Info page helps a DSLAM administrator to identify the model name, firmware / hardware version and MAC address. The screen in [Figure 4-2-1](#) appears.

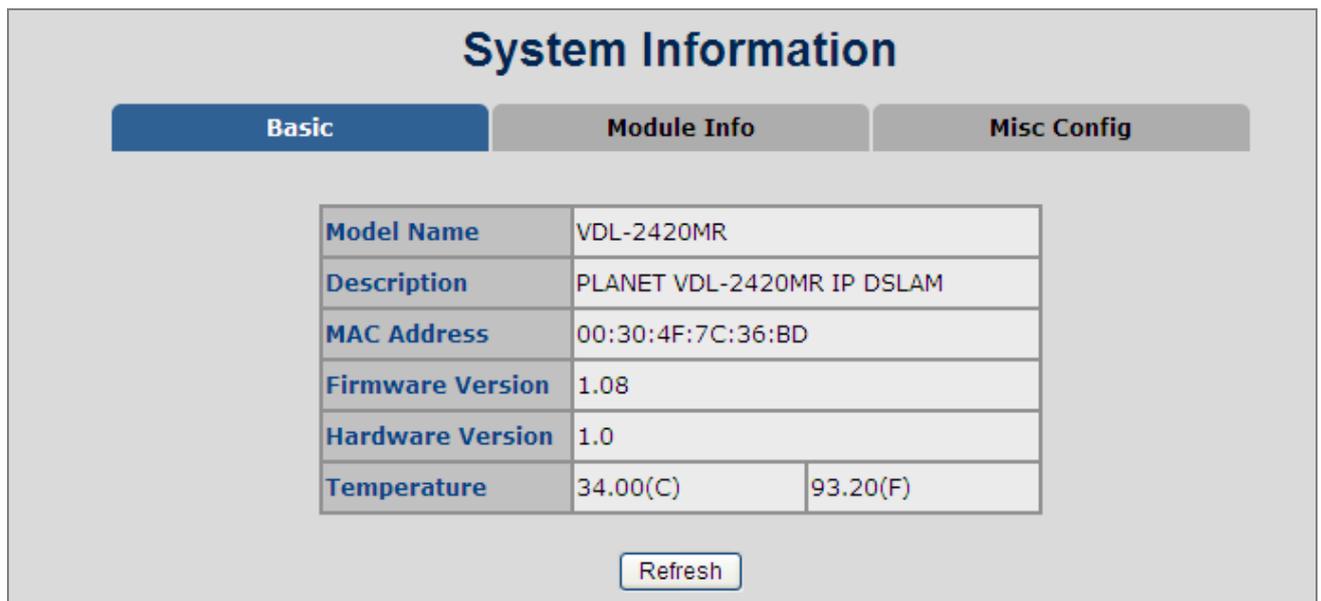


Figure 4-2-1: Basic System Information screenshot

The page includes the following fields:

Object	Description
Model Name:	Display the system name of the IP DSLAM.
Description:	Describes the IP DSLAM.
MAC Address:	Displays the unique hardware address assigned by manufacturer (default).
Firmware Version:	Displays the IP DSLAM's firmware version.
Hardware Version:	Displays the IP DSLAM's hardware version.
Build Firmware Date:	Displays the date information of the firmware.

4.2.1.2 Misc Config

Choose **Misc Config** from System Information of The IP DSLAM, the screen in [Figure 4-2-2](#) appears.

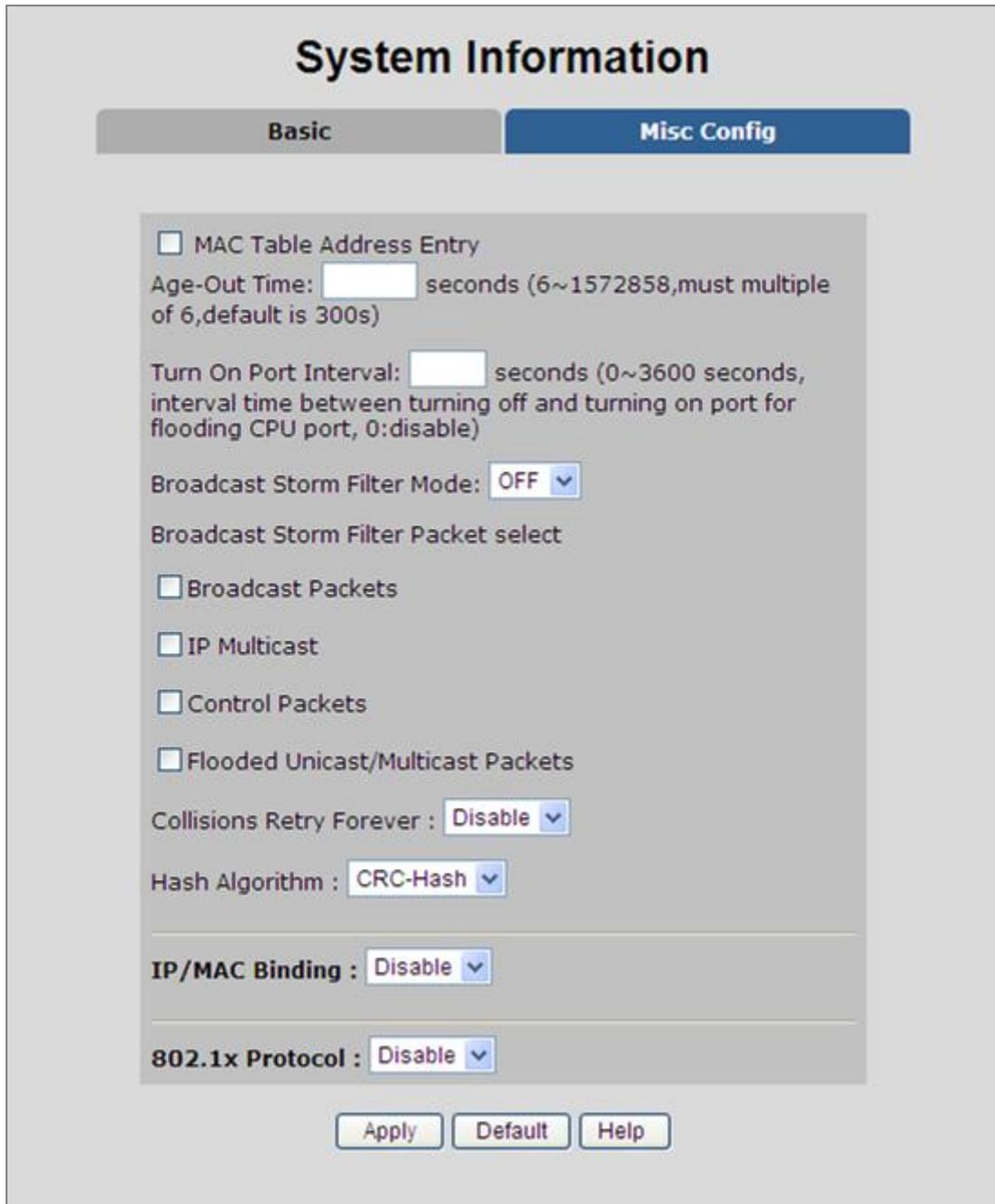


Figure 4-2-2: DSLAM Misc Config screenshot

The page includes the following fields:

Object	Description
MAC Address Age-out Time	Type the number of seconds that an inactive MAC address remains in the IP DSLAM's address table. The value is a multiple of 6. Default is 300 seconds.
Broadcast Storm Filter	To configure broadcast storm control, enable it and set the upper threshold for

Mode	individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 1/2 , 1/4 , 1/8 , 1/16 and OFF . Default is " OFF ".
Broadcast Storm Filter Packets Select	To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. The selectable items as below: <ul style="list-style-type: none"> • Broadcast Packets • IP Multicast • Control Packets • Flooded Unicast / Multicast Packets
Collision Retry Forever	Provide Collision Retry Forever function" Disable " or 16 , 32 , 48 collision numbers on The IP DSLAM. If this function is disabled, when a packet meet a collision, the IP DSLAM will retry 6 times before discard the packets. Otherwise, the IP DSLAM will retry until the packet is successfully sent. Default value is 16 .
Hash Algorithm	Provide MAC address table Hashing setting on The IP DSLAM; available options are CRC-Hash and DirectMap . Default mode is CRC-Hash .
IP/MAC Binding	Enable / Disable IP MAC Binding function.
802.1x protocol	Enable / Disable 802.1x protocols.
Apply button	Press the button to complete the configuration.

4.2.1.3 Module Info

This section provides current status of power supply unit from VDL-2420MR series, the screen in [Figure 4-2-3](#) appears and [table 4-2-1](#) describes the power and fan module Status object of VDL-2420MR series.

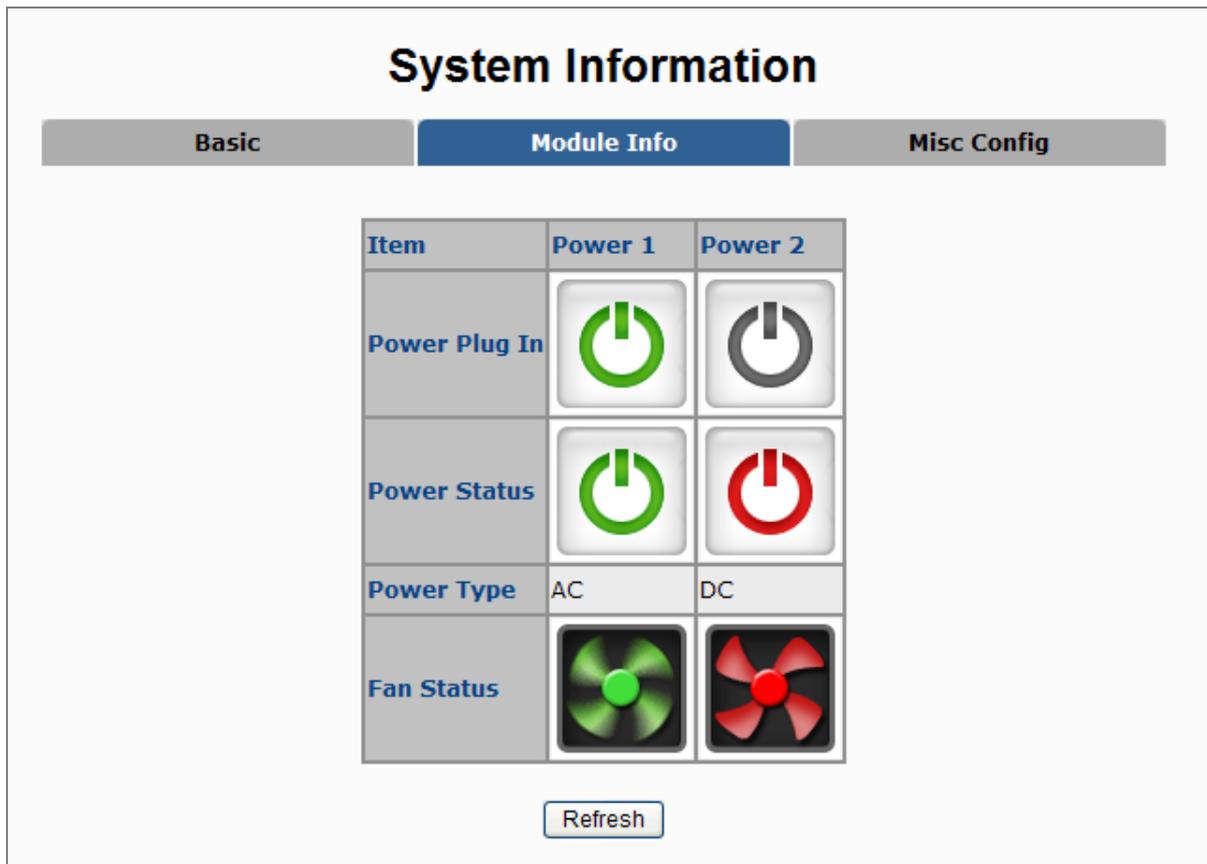


Figure 4-2-3 Chassis Status Web Page Screen

Item	Power 1	Power 2
Power on	<p>Gray: indicate the power supply unit not install into the VDL-2420MR series.</p> <p>Green: indicate the power supply unit install into the VDL-2420MR series.</p>	
Power Status	<p>Gray: indicate the power supply unit not install into the VDL-2420MR series.</p> <p>Green: indicate the power supply unit has power.</p> <p>Red: indicate the power supply unit has no power or failure.</p>	
Power Type	<p>AC: indicate the AC power supply unit (VC-RPS200) install into the VDL-2420MR series.</p> <p>DC: indicate the DC power supply unit (VC-RPS48) install into the VDL-2420MR series.</p>	
Fan Status	<p>Gray: indicate the power supply unit not install into the VDL-2420MR series.</p> <p>Green: indicate the fan is operation normally.</p> <p>Red: indicate the fan is failure.</p>	

Table 4-2-1 Descriptions of the Chassis Status Web Page Screen Objects



Once, installed the AC or DC power supply unit into VDL-2420MR series, the fan will start to working. Even, the AC or DC power supply unit has no power.

4.2.2 IP Configuration

The IP DSLAM is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the IP DSLAM.

IP address overview

What is an IP address?

Each device (such as a computer) which participates in an IP network needs a unique "address" on the network. It's similar to having a US mail address so other people have a know way to send you messages. An IP address is a four byte number, which is usually written in "dot notation" - each of the bytes' decimal value is written as a number, and the numbers are separated by "dots" (aka periods). An example: 199.25.123.1

How do I get one for this box?

The IP addresses on most modern corporate nets are assigned by an employee called a "Network Administrator", or "Sys. Admin". This person assigns IP addresses and is responsible for making sure that IP addresses are not duplicated - If this happens one or both machines with a duplicate address will stop working.

Another possibility is getting your address assigned to you automatically over the net via DHCP protocol. Enable DHCP function, and reset the machine. If your network is set up for this service, you will get an IP address assigned over the network. If you don't get an address in about 30 seconds, you probably don't have DHCP.

■ IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in [Figure 4-2-4](#) appears.

The screenshot shows a web-based configuration interface titled "IP Configuration". At the top, there is a "DHCP:" label followed by a dropdown menu currently set to "Disable". Below this, there is a table with three rows for configuration fields:

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254

At the bottom of the interface, there are two buttons: "Apply" and "Help".

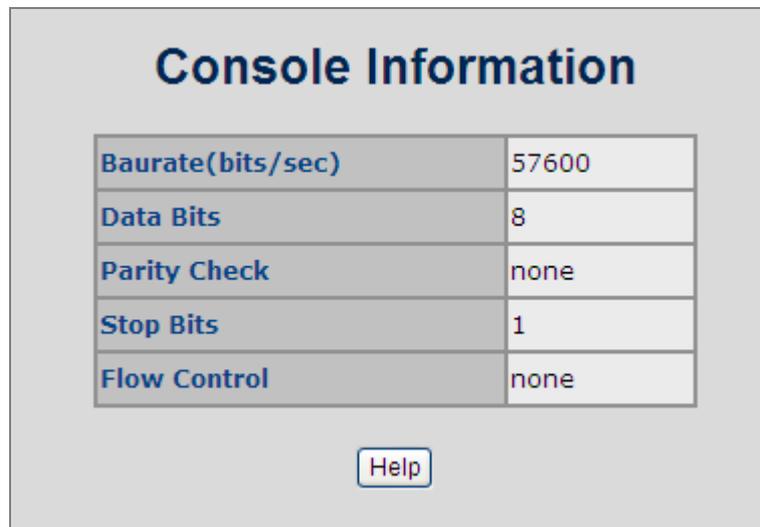
Figure 4-2-4: IP configuration interface

The page includes the following fields:

Object	Description
DHCP	<p>Enable or disable the DHCP client function.</p> <p>When DHCP function is enabled, the IP DSLAM will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.</p>
IP Address	<p>Assign the IP address that the network is using.</p> <p>If DHCP client function is enabled, this DSLAM is configured as a DHCP client. The network DHCP server will assign the IP address to the IP DSLAM and display it in this column.</p> <p>The default IP is 192.168.0.100 or the user has to assign an IP address manually when DHCP Client is disabled.</p>
Subnet Mask	<p>Assign the subnet mask to the IP address.</p> <p>If DHCP client function is disabled, the user has to assign the subnet mask in this column field.</p>
Gateway	<p>Assign the network gateway for the IP DSLAM.</p> <p>If DHCP client function is disabled, the user has to assign the gateway in this column field.</p> <p>The default gateway is 192.168.0.254.</p>

4.2.3 Console Information

Console is a standard UART interface to communicate with Serial Port. You can use Windows HyperTerminal program to link the IP DSLAM. The page displays the required console settings on the IP DSLAM.



Console Information	
Baurate(bits/sec)	57600
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

Help

Figure 4-2-5: Console Information interface

4.2.4 SNMP Configuration

4.2.4.1 SNMP Overview

The **Simple Network Management Protocol (SNMP)** is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol :

- **Network management stations (NMSs)** : Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents** : Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** : A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol** : A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get** -- Allows the NMS to retrieve an object instance from the agent.
- **Set** -- Allows the NMS to set values for object instances within an agent.
- **Trap** -- Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. The normal SNMP default communities are as below when configured:

- Write = **private**
- Read = **public**

4.2.4.2 System Options

Use this page to define management stations. You can also define a name, location, and contact person for the IP DSLAM.

The image shows a web-based configuration interface titled "SNMP Configuration" with a sub-section "System Options". It contains four input fields: "Name:" with the value "VDL-2420MR", "Location:" with "No Location", "Contact:" with "No Contact", and "SNMP Status:" with a dropdown menu set to "Enable". Below the fields are "Apply" and "Help" buttons.

Figure 4-2-6: SNMP configuration interface

The page includes the following fields:

Object	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor).
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person.
SNMP Status	Indicates the SNMP mode operation. Possible modes are:

- **Enabled:** Enable SNMP mode operation.
- **Disabled:** Disable SNMP mode operation.

4.2.4.3 Community Strings

Community strings serve as passwords and can be entered as one of the following:



Figure 4-2-7: Community strings interface

The page includes the following fields:

Object	Description
Community Strings:	<p>Here you can define the new community string set and remove the unwanted community string.</p> <ul style="list-style-type: none"> ■ String: Fill the name string. ■ RO: Read only. Enables requests accompanied by this community string to display MIB-object information. ■ RW: Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
 button	Press the button to add the management SNMP community strings on the IP DSLAM.
 button	Press the button to remove the management SNMP community strings that you defined before on the IP DSLAM.

4.2.4.4 Trap Managers

A trap manager is a management station that receives the trap messages generated by the IP DSLAM. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.



Figure 4-2-8: Trap Managers interface

The page includes the following fields:

Object	Description
IP Address:	Enter the IP address of the trap manager.
Community:	Enter the community string for the trap station.

4.2.4.5 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.

The SNMPv3 Groups Configuration screen in [Figure 4-2-9](#) appears.

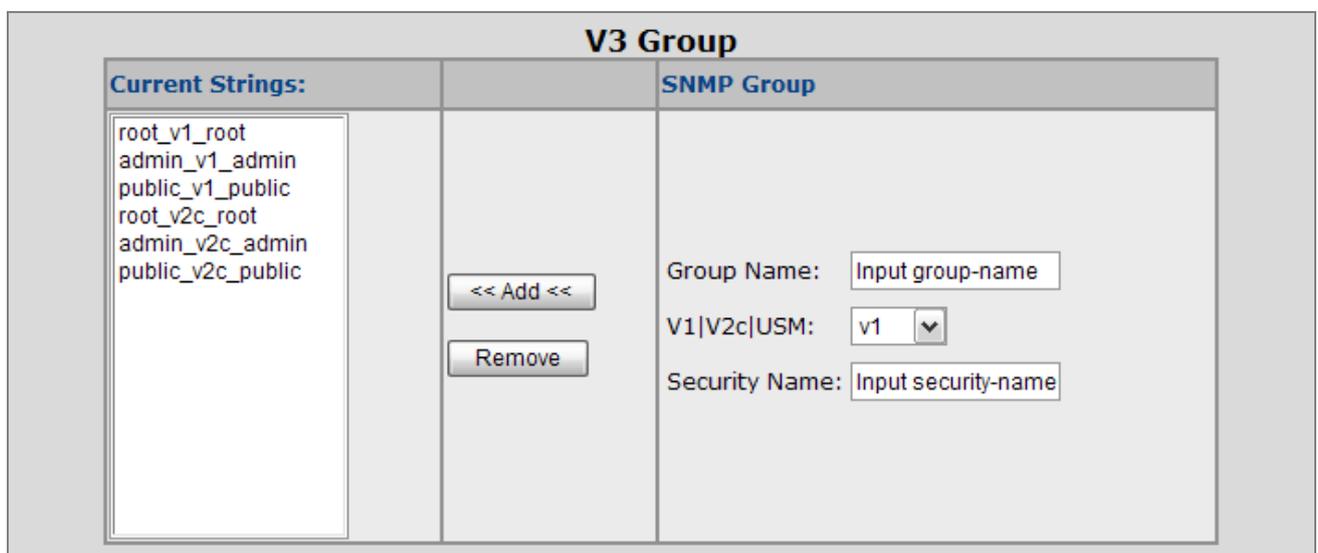


Figure 4-2-9: SNMP configuration interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 V2c USM	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> • v1: Reserved for SNMPv1. • v2c: Reserved for SNMPv2c. • usm: User-based Security Model (USM).
Security Name:	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 15.
Remove	Check to delete the entry. It will be deleted during the next save.

4.2.4.6 SNMPv3 View

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.

The SNMPv3 Views Configuration screen in [Figure 4-2-10](#) appears.

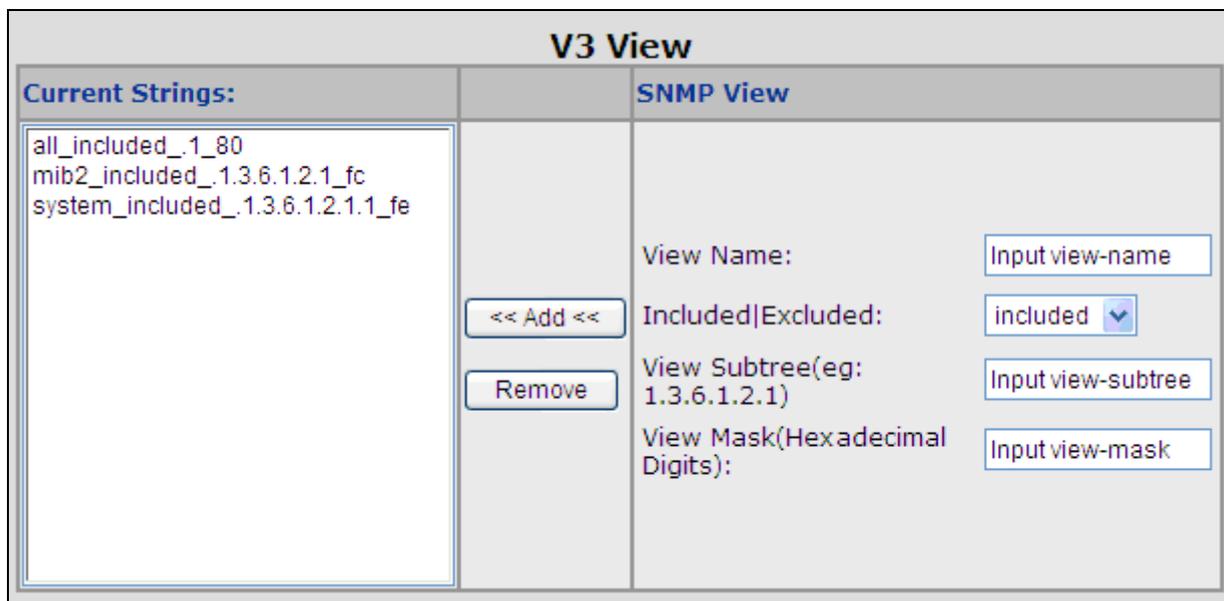


Figure 4-2-10: SNMP configuration interface

The page includes the following fields:

Object	Description
View Name:	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 15.
Included Excluded:	Indicates the view type that this entry should belong to. Possible view type are:

	<ul style="list-style-type: none"> • included: An optional flag to indicate that this view subtree should be included. • excluded: An optional flag to indicate that this view subtree should be excluded.
View Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*)
View Mask(Hexadecimal Digits):	View mask is defined in order to reduce the amount of configuration information required when fine-grained access control is required (e.g., access control at the object instance level)

4.2.4.7 SNMPv3 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level. The SNMPv3 Accesses Configuration screen in [Figure 4-2-11](#) appears.

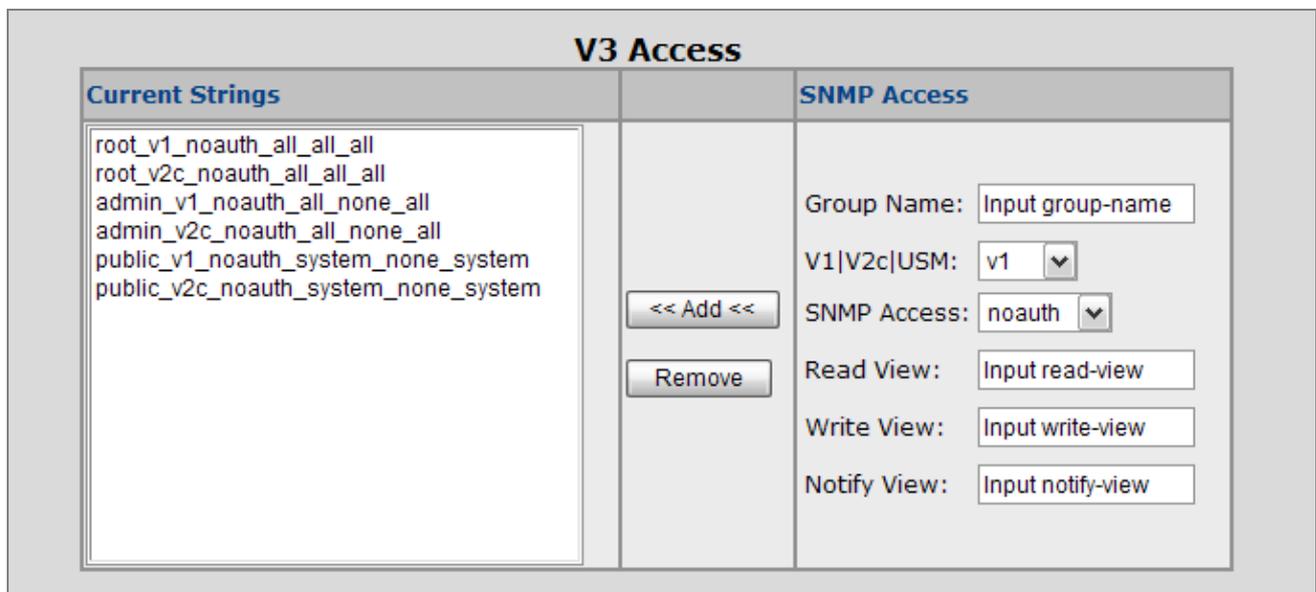


Figure 4-2-11: SNMP configuration interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 V2c USM:	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> • v1: Reserved for SNMPv1. • v2c: Reserved for SNMPv2c. • usm: User-based Security Model (USM)
SNMP Access:	Indicates the security model that this entry should belong to. Possible security models are:

	<ul style="list-style-type: none"> • NoAuth: None authentication and none privacy. • Auth: Authentication and none privacy. • Authpriv: Authentication and privacy.
Read View:	<p>The name of the MIB views defining the MIB objects for which this request may request the current values.</p> <p>The allowed string length is 1 to 16.</p>
Write View:	<p>The name of the MIB views defining the MIB objects for which this request may potentially SET new values.</p> <p>The allowed string length is 1 to 16.</p>
Notify View:	Set up the notify view.
Add button	Press the button to add the management SNMP community strings on the IP DSLAM.
Remove button	Check to delete the selected entry. It will be deleted during the next save.

4.2.4.8 SNMP V3 usm-user

Configure SNMPV3 users table on this page. The entry index keys are Engine ID and User Name.

The SNMPV3 Users Configuration screen in [Figure 4-2-12](#) appears.

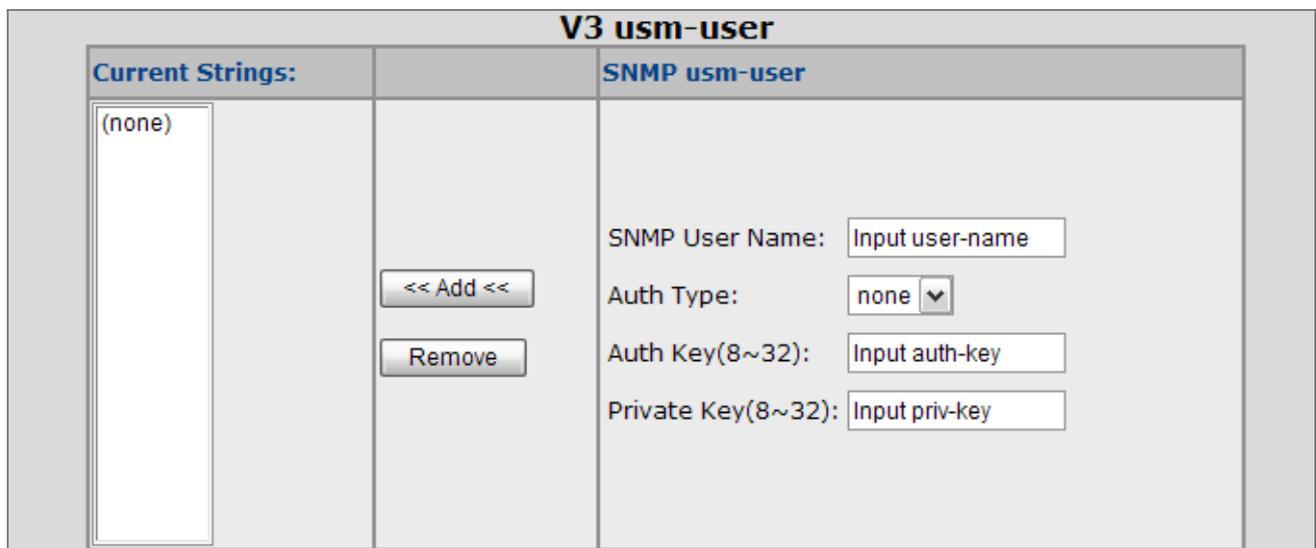


Figure 4-2-12: SNMP configuration interface

The page includes the following fields:

Object	Description
SNMP User Name:	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 15.
Auth Type:	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are:

-
- **None:** None authentication protocol.
 - **MD5:** An optional flag to indicate that this user using MD5 authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Auth Key(8~32):

A string identifying the authentication pass phrase.

For MD5 authentication protocol, the allowed string length is 8 to 32.

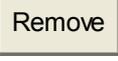
Private Key(8~32):

A string identifying the privacy pass phrase.

The allowed string length is 8 to 32.

 **button**

Press the button to add the management SNMP community strings on the IP DSLAM.

 **button**

Check to delete the selected entry. It will be deleted during the next save.

4.2.5 Syslog Setting

The Syslog Setting page allows you to configure the logging of messages that are sent to remote syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

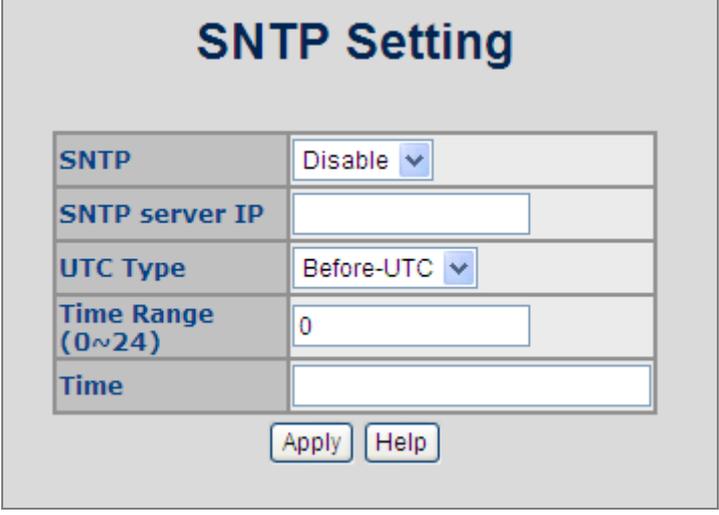
Figure 4-2-13: Syslog Setting web interface

The page includes the following fields:

Object	Description
Syslog Server IP	IP address of syslog server.
Log level	<ul style="list-style-type: none"> • None: No send syslog message to syslog server, and Max Age parameters of the root bridge, regardless of how it is configured. • Major: only send major syslog to syslog server, eg: link up/down, system warm/cold start • All: send all syslog messages to syslog server.

4.2.6 SNTP Setting

The Simple Network Time Protocol (SNTP) allows user could configure the IP DSLAM to send time synchronization requests to specific time servers (i.e., client mode) by IP address.



The screenshot shows the 'SNTP Setting' web interface. It features a title 'SNTP Setting' at the top. Below the title is a form with five rows of settings:

- SNTP**: A dropdown menu currently set to 'Disable'.
- SNTP server IP**: An empty text input field.
- UTC Type**: A dropdown menu currently set to 'Before-UTC'.
- Time Range (0~24)**: A text input field containing the number '0'.
- Time**: An empty text input field.

At the bottom of the form are two buttons: 'Apply' and 'Help'.

Figure 4-2-14: SNTP Setting web interface

The page includes the following fields:

Object	Description
SNTP	Enable or Disable SNTP Feature.
SNTP server IP	Allows to assign a SNTP sever IP address here.
UTC Type	Allows user to select time zone. Ex. If your location is in Taipei (UTC+08) then You have to choose After-UTC. If your location is in San Francisco (UTC-08) then you have to choose Before-UCT.
Time Range (0~24)	Allows user input time range. Ex. if time zone is UTC+08 is then input 8, if time zone is UTC-05 then input 5.
Time	Shows current time after connected to NTP server.

4.2.7 Firmware Upgrade

It provides the functions allowing the user to update the IP DSLAM firmware via the **Trivial File Transfer Protocol (TFTP)** server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

4.2.7.1 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the IP DSLAM firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in [Figure 4-2-15](#) appears.

Use this menu to download a file from specified TFTP server to the IP DSLAM.

The screenshot shows a web interface titled "Firmware Upgrade" with a subtitle "TFTP Firmware Upgrade". It contains two input fields: "TFTP Server IP Address" with the value "192.168.0.1" and "Firmware File Name" with the value "VDL-2420MR.img". Below the fields are two buttons: "Apply" and "Help".

Figure 4-2-15: Firmware Upgrade interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in your TFTP server IP.
Firmware File Name:	Type in the name of the firmware image file to be updated.

4.2.7.2 HTTP Firmware Upgrade

The **HTTP Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in [Figure 4-2-16](#) appears.



Figure 4-2-16: HTTP Firmware Upgrade interface

To open **Firmware Upgrade** screen perform the following:

1. Click System -> Web Firmware Upgrade.
2. The Firmware Upgrade screen is displayed as in [Figure 4-2-17](#).
3. Click the "Browse" button of the main page, the system would pop up the file selection menu to choose firmware.

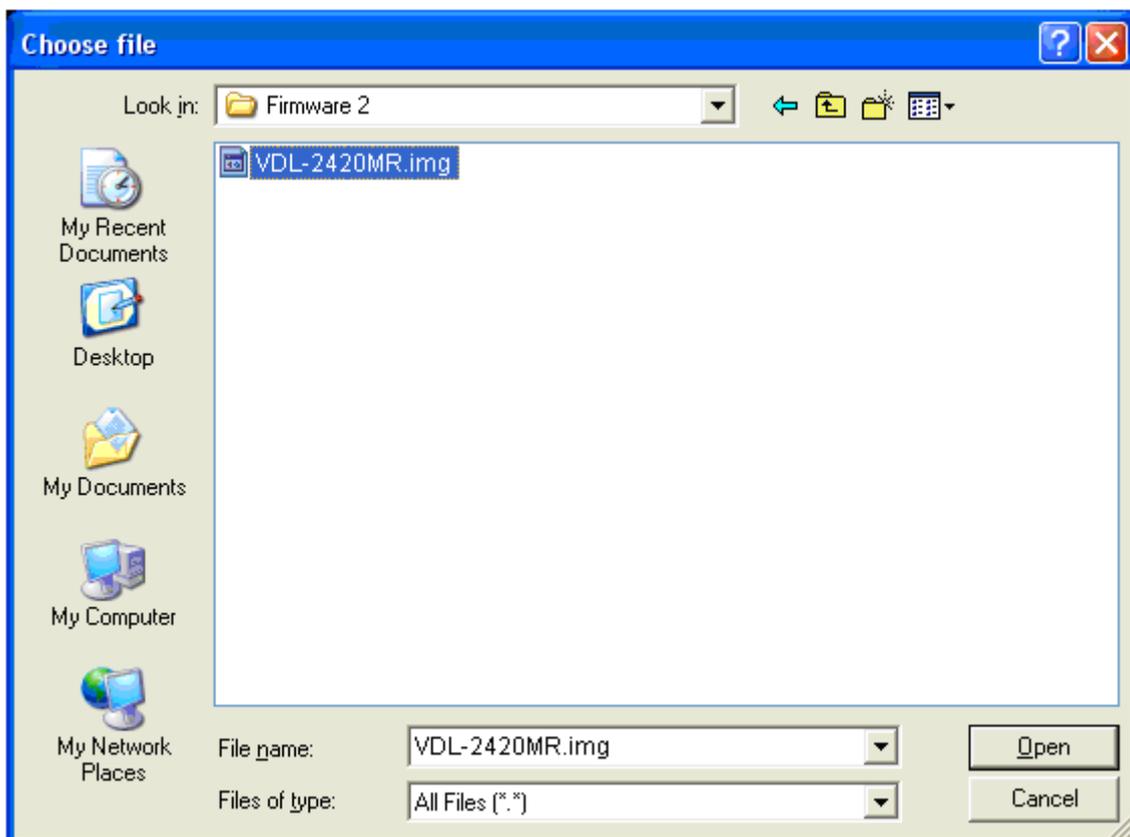


Figure 4-2-17: HTTP Firmware Upgrade selection window

- Select on the firmware then click “**Submit**”, the Software Upload Progress would show the file upload status.



Firmware upgrade needs several minutes. Please wait a while, and then manually refresh the webpage.

4.2.8 Configuration Backup

4.2.8.1 TFTP Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the IP DSLAM will download back the flash image.

Figure 4-2-18: TFTP Configuration Restore interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Restore File Name:	Type in the correct file name for restoring.

4.2.8.2 HTTP Config File Restore

You can also restore the previous backup configuration from the current workstation utilize internet browser such as Microsoft Internet Explore or Mozilla Firefox, to recover the settings. Before doing that, you must locate the image file on the local management station first and the IP DSLAM will download back the flash image

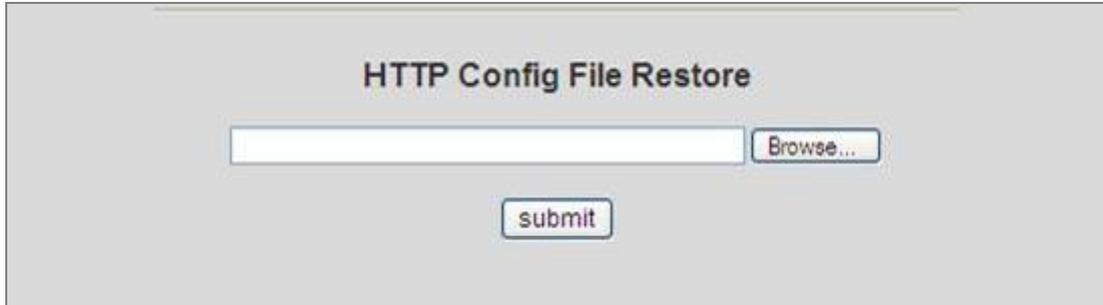


Figure 4-2-19: HTTP Configuration Restore interface

4.2.8.3 TFTP Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

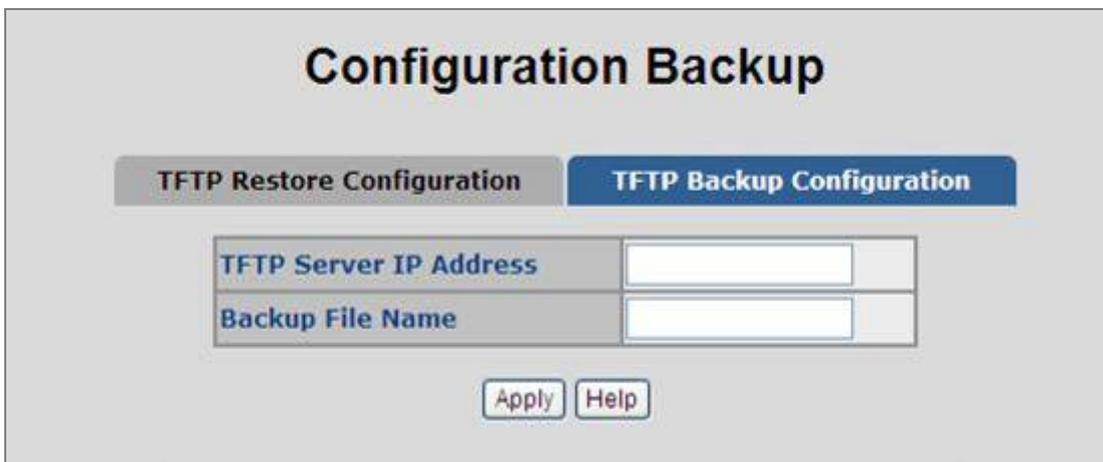


Figure 4-2-20: TFTP Configuration Backup interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Backup File Name:	Type in the file name that will backup on the TFTP server.

4.2.8.4 HTTP Config File Backup

This function allows backup the current configuration of the IP DSLAM to the local management station. The screens in [Figure 4-2-21](#) and [Figure 4-2-22](#) appear.

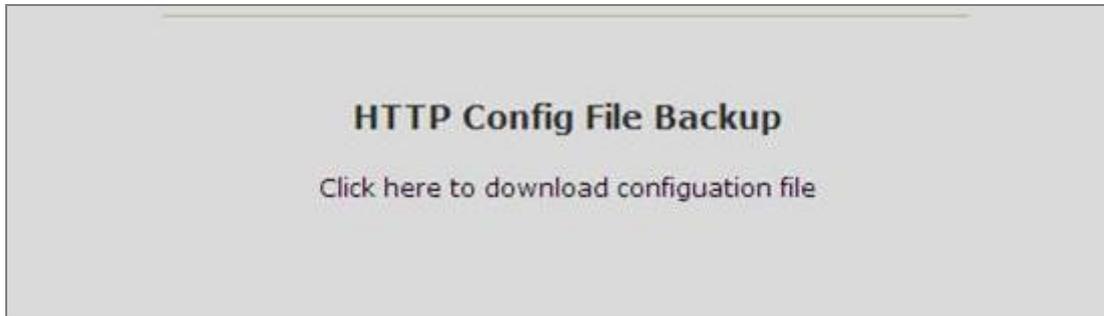


Figure 4-2-21: HTTP configuration file backup interface

Move the cursor to “Click here to download configuration file” and click. The backup configuration file will be packaged as a “config.tar” file as default.

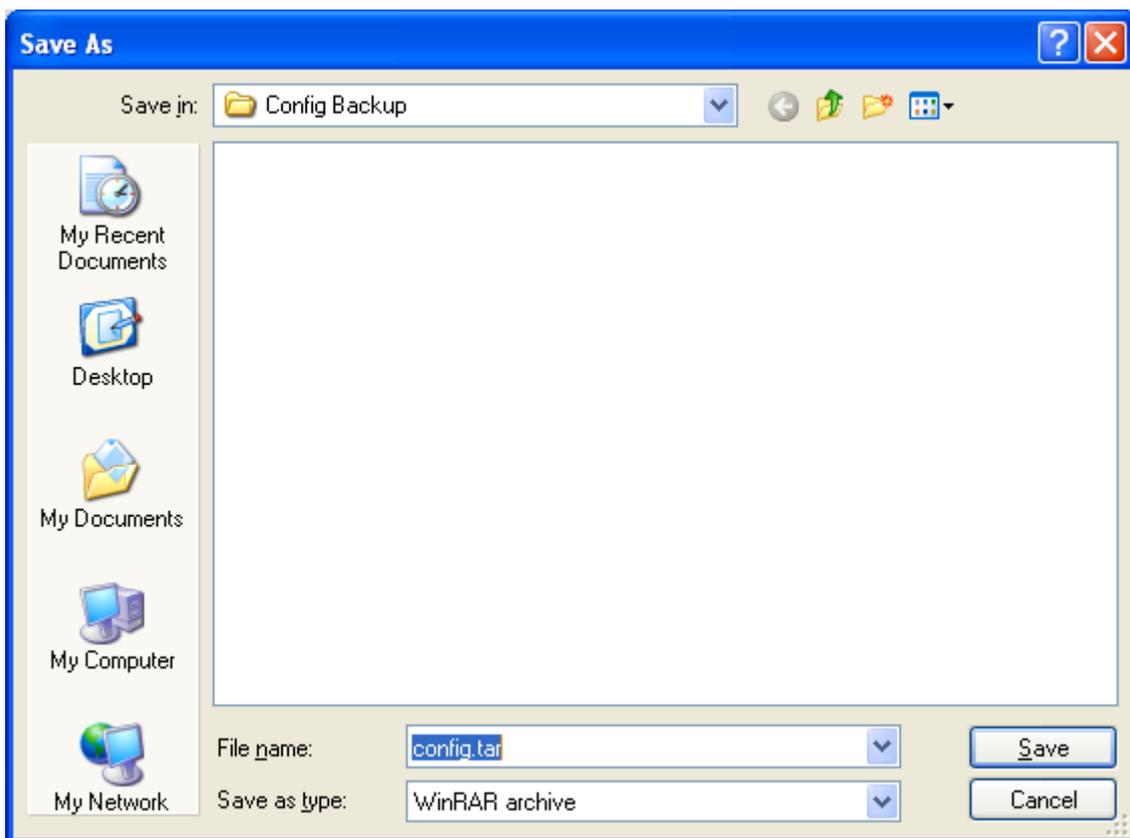


Figure 4-2-22: HTTP Configuration Backup window

4.2.9 Factory Default

Reset DSLAM to default configuration. Click to reset all configurations to the default value.

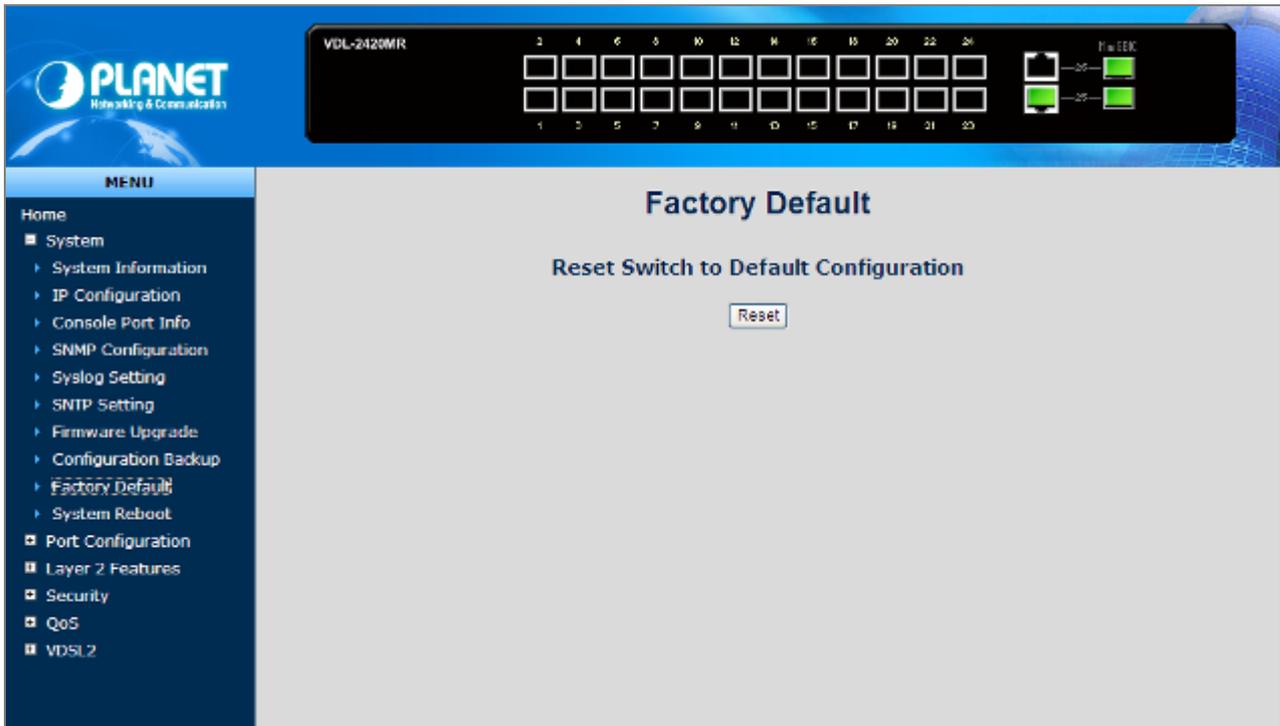


Figure 4-2-23: Factory Default interface

4.2.10 System Reboot

Reboot the IP DSLAM in software reset. Click to reboot the system.

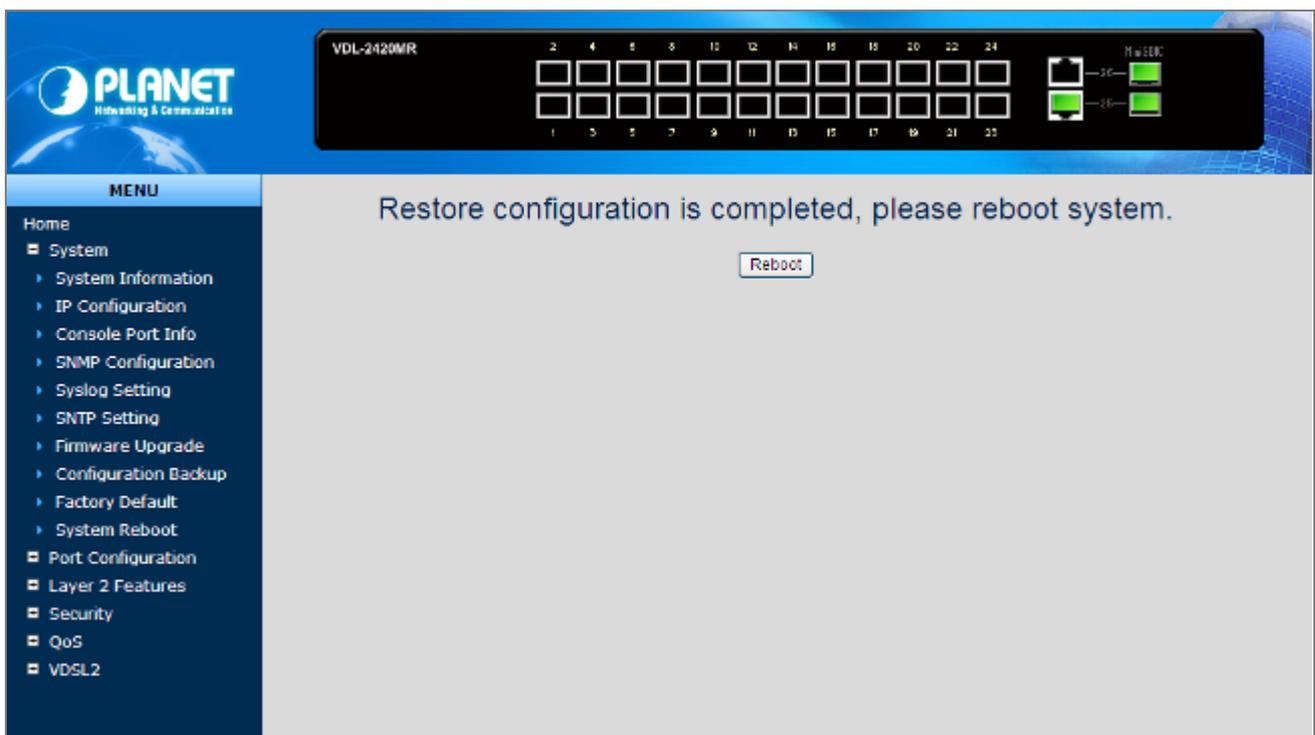


Figure 4-2-24: System Reboot interface

4.3 Port Configuration

Use the Port Configuration Menu to display or configure the IP DSLAM's ports. This section has the following items:

- **Port Control** Configures port connection settings
- **Port Status** Display the current Port link status and speed etc.
- **Port Statistics** Lists Ethernet and RMON port statistics
- **Port Sniffer** Sets the source and target ports for mirroring
- **Protected Port** Configures Protected Ports and groups

4.3.1 Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
						Ingress	Egress			
Port1	Enable	Auto	1000	Full	Enable	0	0	<input type="checkbox"/>	Enable	Enable
Port2										
Port3										
Port4										

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			

Figure 4-3-1: Port Control interface

The page includes the following fields:

Object	Description
Port:	Use the scroll bar and click on the port number to choose the port to be configured.
State:	Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
Negotiation:	The item is only for Gigabit ports of the IP DSLAM. Auto and Force . Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
Speed:	The item is only for Gigabit ports of the IP DSLAM. It is available for selecting when the Negotiation column is set as Force. When

	the Negotiation column is set as Auto, this column is read-only.
	The item is only for Gigabit ports of the IP DSLAM.
Duplex:	It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Flow Control:	Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
	The item is only for Gigabit ports of the IP DSLAM.
	Supports by-port ingress and egress rate control.
	For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.
Rate Control: (Unit: 128KBbps)	<ul style="list-style-type: none"> ■ Ingress: Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~ 8000: valid rate value ■ Egress: Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~8000: valid rate value.
Security:	<p>A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally.</p> <p>User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click Apply button to change on this page.</p>
BSF:	<p>User can disable/Enable port broadcast storm filtering option by port.</p> <p>The filter mode and filter packets type can be select in DSLAM Setting > Misc Config page.</p>
Jumbo Frame:	User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet.

4.3.2 Port Status

This page displays current port configurations and operating status - it is a ports' configurations summary table. Via the summary table, you can know status of each port clear at a glance, like Port Link Up/Link Down status, negotiation, Link Speed, Rate Control, Duplex mode and Flow Control.

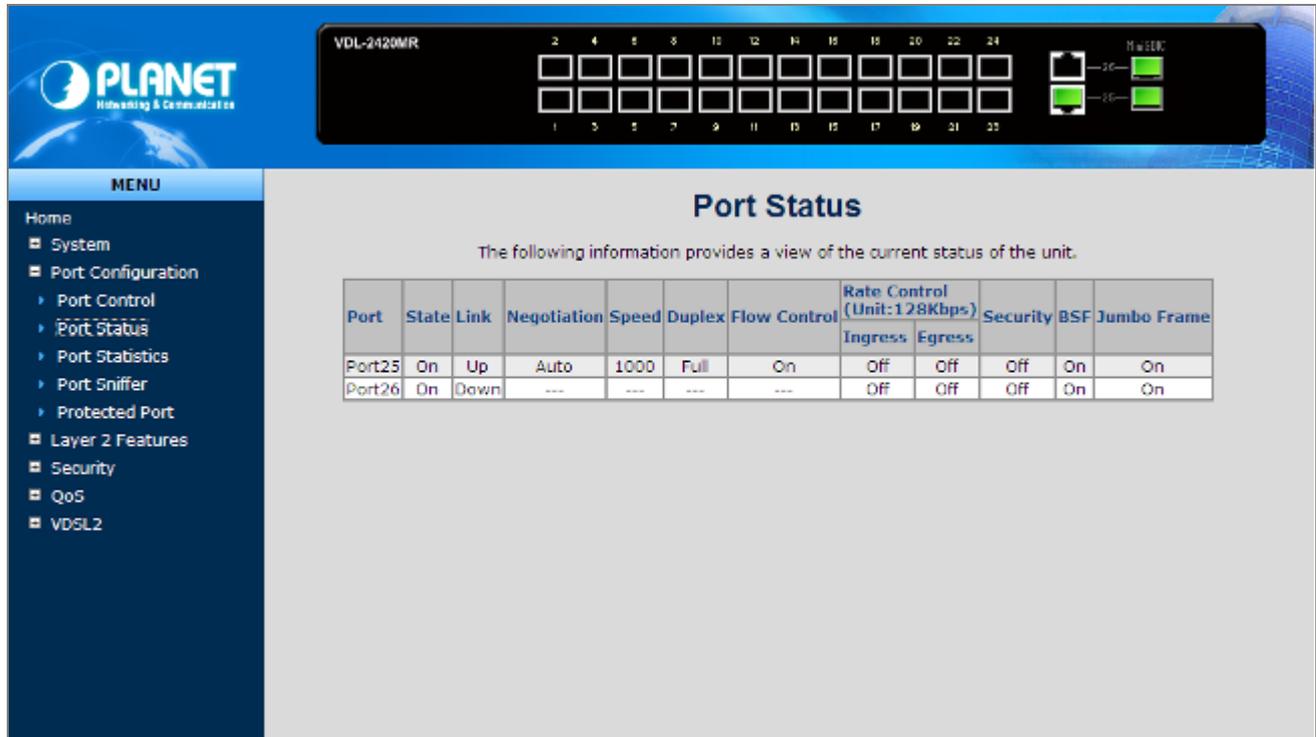


Figure 4-3-2: Port Status interface

4.3.3 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

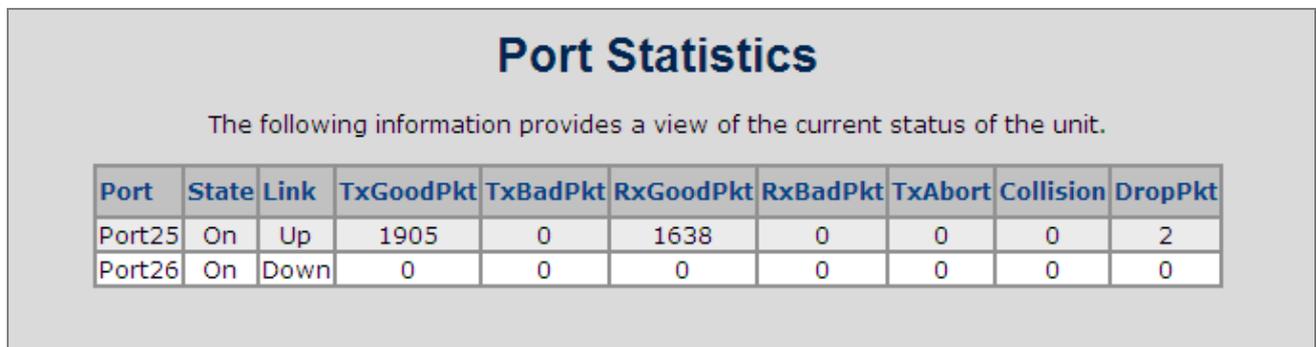


Figure 4-3-3: Port Statistics interface

The page includes the following fields:

Object	Description
Port:	The port number.
State:	It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
Link:	The status of linking—'Up' or 'Down'.
Tx Good Packet:	The counts of transmitting good packets via this port.
Tx Bad Packet:	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
Rx Good Packet:	The counts of receiving good packets via this port.
Rx Bad Packet:	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet:	The aborted packet while transmitting.
Packet Collision:	The counts of collision packet.
Packet Dropped:	The counts of dropped packet.

4.3.4 Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

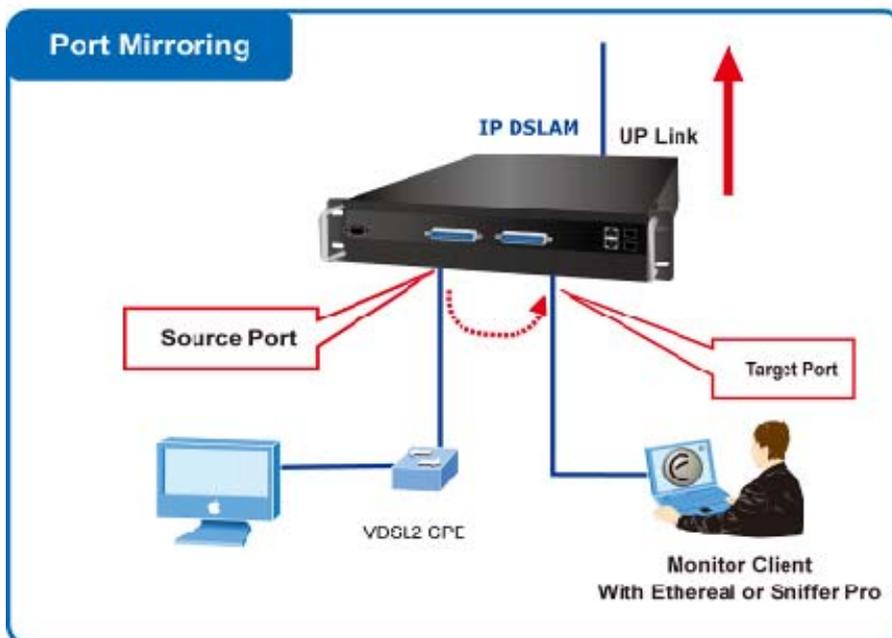


Figure 4-3-4: Port Mirror application

Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those packets will be sent.

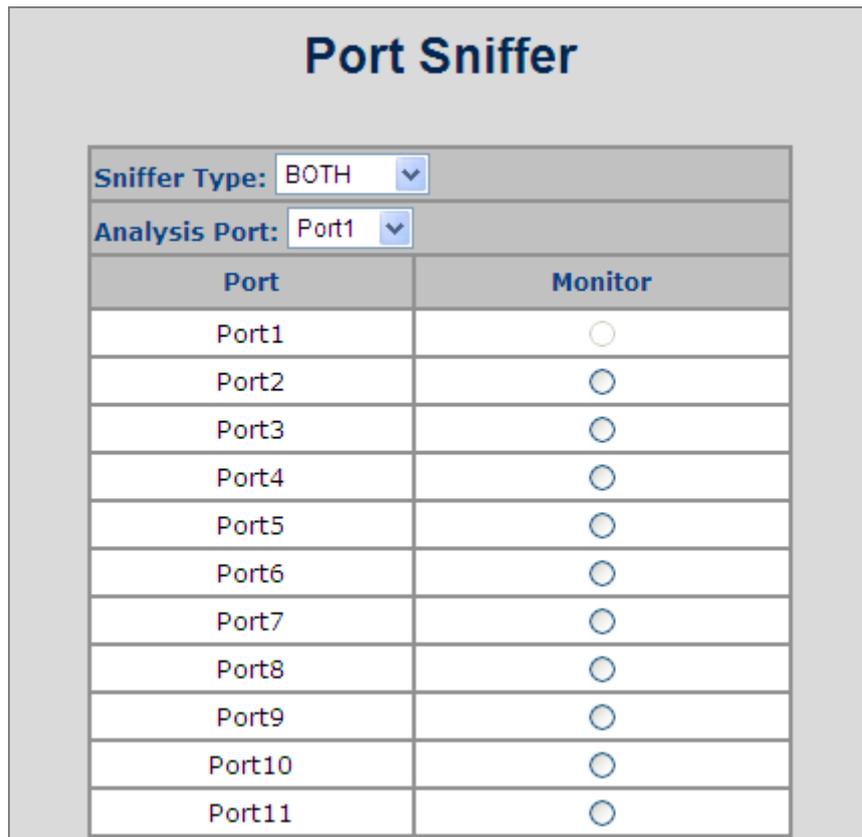


Figure 4-3-5: Port Sniffer interface

The page includes the following fields:

Object	Description
Sniffer Type:	Select a sniffer mode: <ul style="list-style-type: none"> • DISABLE • RX • TT • BOTH
Analysis (Monitoring) Port:	It' means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer or netxray.
Monitored Port:	The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the IP DSLAM. User can choose which port that they want to monitor in only one sniffer type.



- 1 When the Mirror Mode set to **RX** or **TX** and the **Analysis Port** be selected, the packets to and from the **Analysis Port** will not be transmitted. The Analysis Port will accept only COPIED packets from the **Monitored Port**.
- 2 If you want to disable the function, you must select monitor port to none.

4.3.5 Protect Port

There are two protected port groups; ports in different groups can't communicate.

In the same group, protected ports can't communicate with each other, but can communicate with unprotected ports.

Unprotected ports can communicate with any ports, including protected ports.

Protected Port Setting			
Port ID	Protected	Group1	Group2
Port1	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port4	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port5	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port6	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port7	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port8	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port9	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port10	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port11	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port12	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port13	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>

Figure 4-3-6: Protected Port Setting Web interface

The page includes the following fields:

Object	Description
Port ID	Identify the IP DSLAM interface.
Protected	Enable the Protected function on the selected port. If the check box is not shown as <input checked="" type="checkbox"/> , then this port a unprotected port and it can communicate with any ports - including protected ports
Group 1	Set the protected port to be Group 1 member.
Group 2	Set the protected port to be Group 2 member.



Usually, set the **Uplink port** or the Port is connected to Core DSLAM or router to be the **Un-protected port**.

4.4 VLAN configuration

4.4.1 VLAN Overview

A **Virtual Local Area Network (VLAN)** is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.



-
1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
 2. The IP DSLAM supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
-

The IP DSLAM supports **IEEE 802.1Q (tagged-based)** and **Port-Base VLAN** setting in web management page. In the default configuration, VLAN support is “**802.1Q**”.

■ Port-based VLAN

Port-based VLAN limit traffic that flows into and out of DSLAM ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a DSLAM, or an entire department.

On port-based VLAN, NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another DSLAM port, VLAN considerations come into play to decide if the packet is dropped by the IP DSLAM or delivered.

■ IEEE 802.1Q VLANs

IEEE 802.1Q (tagged) VLAN are implemented on the IP DSLAM. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes

broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

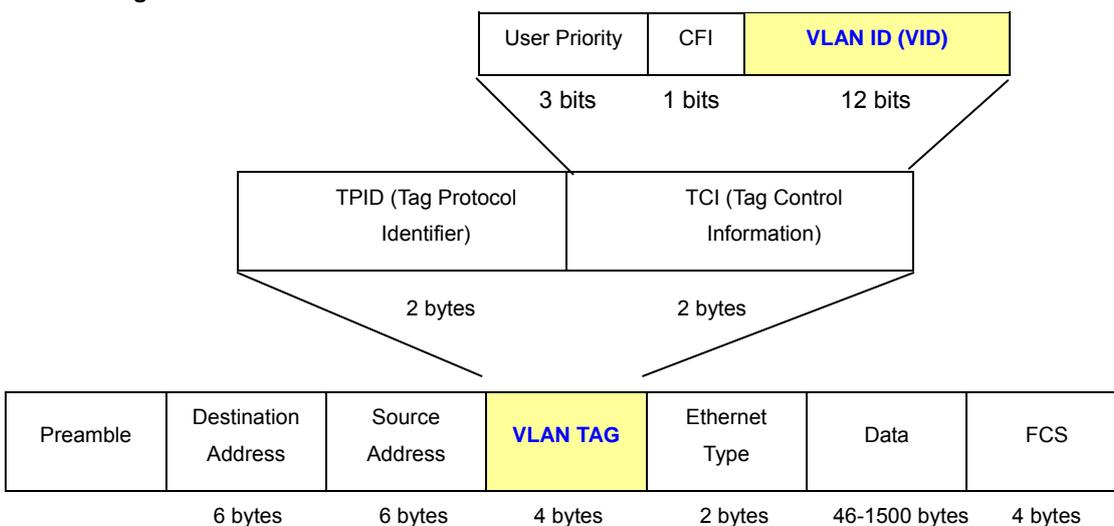
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to **0x8100**, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

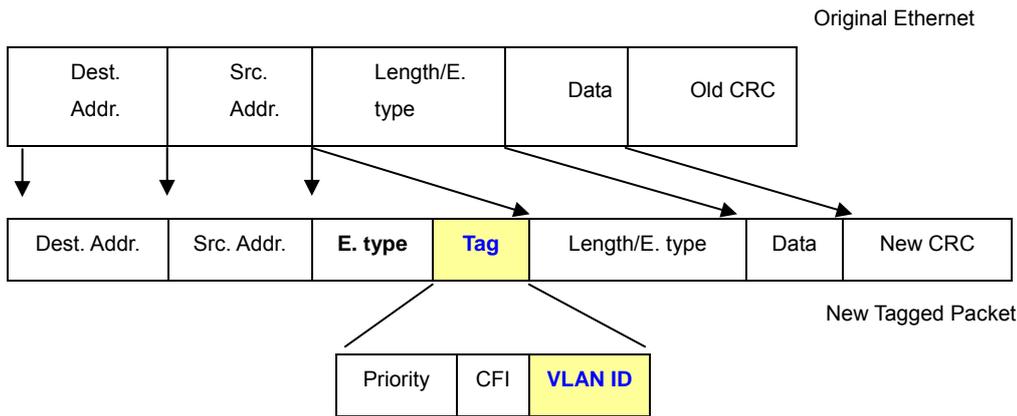
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



■ Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a DSLAM has a PVID. 802.1Q ports are also assigned a PVID, for use within the IP DSLAM. If no VLAN are defined on the IP DSLAM, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the IP DSLAM to VID on the network. The IP DSLAM will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the IP DSLAM will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A DSLAM port can have only one PVID, but can have as many VID as the IP DSLAM has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

■ Default VLANs

The IP DSLAM initially configures one VLAN, VID = 1, called "**default.**" The factory default setting assigns all ports on the IP DSLAM to the "**default.**". As new VLAN are configured in Port-based mode, their respective member ports are removed from the "**default.**"

■ VLAN and Link aggregation Groups

In order to use VLAN segmentation in conjunction with port link aggregation groups, you can first set the port link

aggregation group(s), and then you may configure VLAN settings. If you wish to change the port link aggregation grouping with VLAN already in place, you will not need to reconfigure the VLAN settings after changing the port link aggregation group settings. VLAN settings will automatically change in conjunction with the change of the port link aggregation group settings.

4.4.2 Static VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a DSLAM is logically equivalent of reconnecting a group of network devices to another Layer 2 DSLAM. However, all the network devices are still plug into the same DSLAM physically.

The IP DSLAM supports **Port-based** and **802.1Q (Tagged-based)** VLAN in web management page. In the default configuration, VLAN support is "802.1Q".

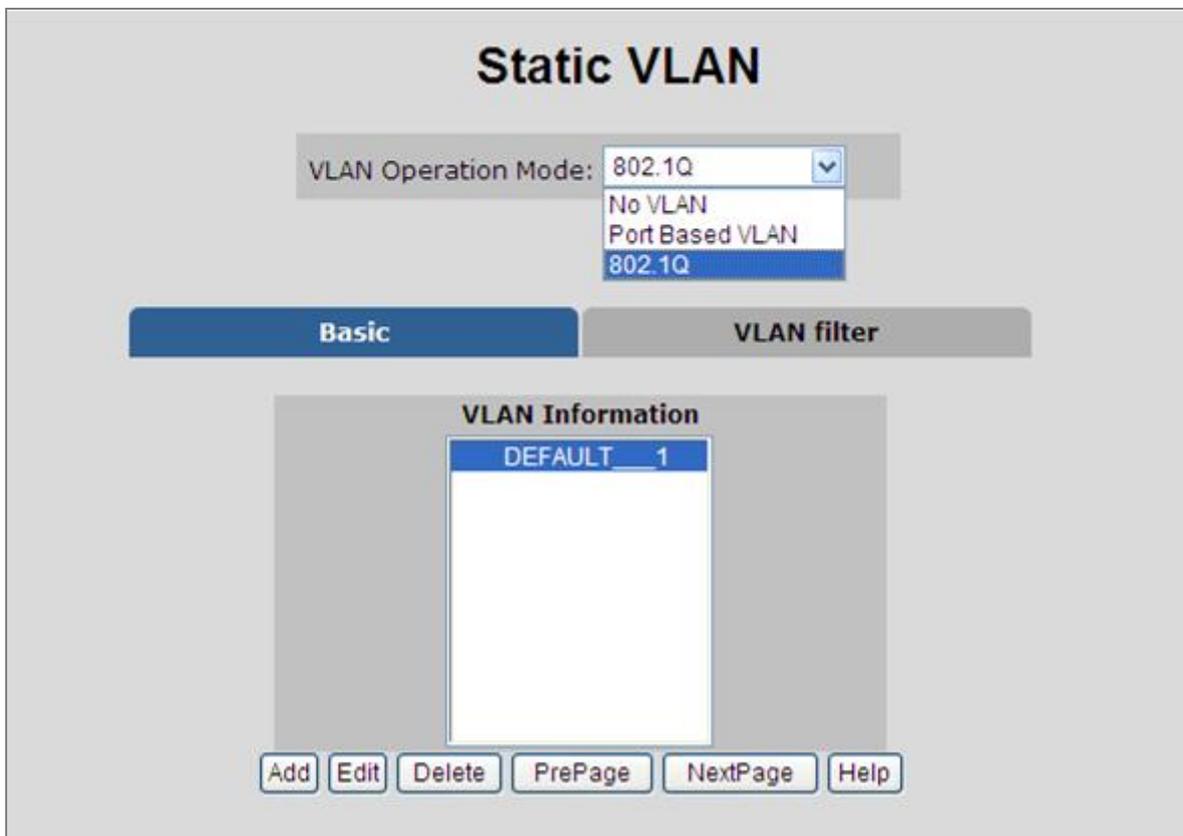


Figure 4-4-1: Static VLAN interface



- 1 No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
- 2 The IP DSLAM supports **Port-based VLAN** and **IEEE 802.1Q VLAN**. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

4.4.3 Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

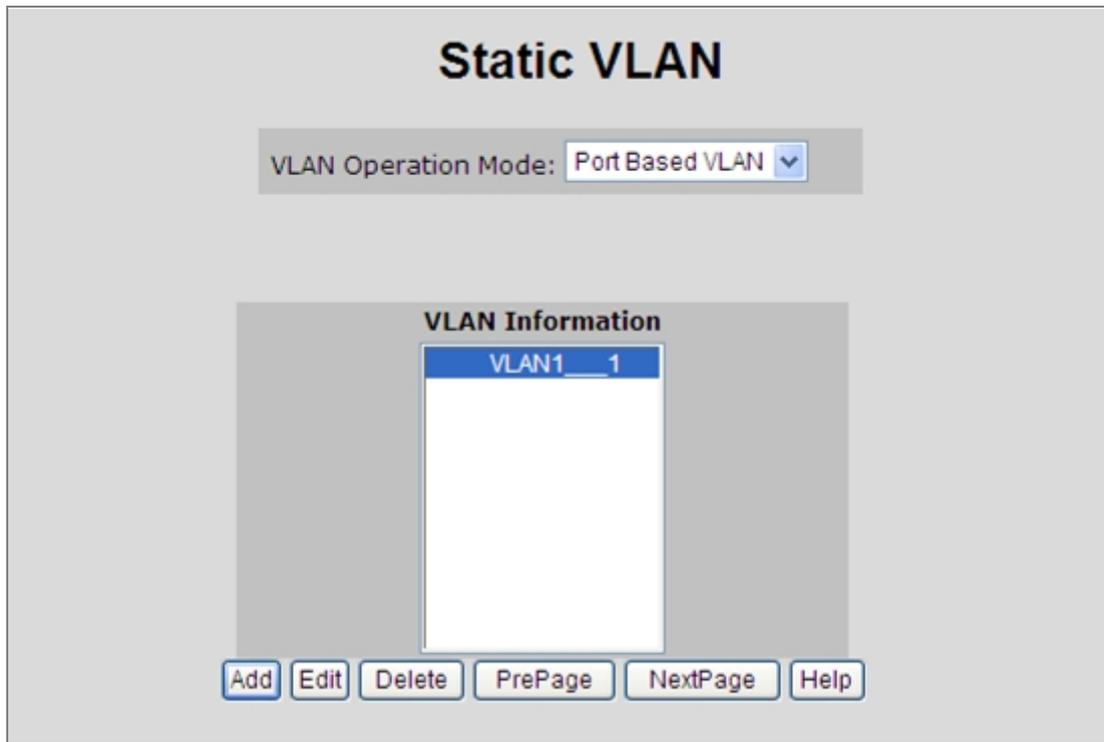


Figure 4-4-2: Port-based VLAN interface

■ Create a VLAN and add member ports to it

1. Click the hyperlink "VLAN" \ "Static VLAN" to enter the VLAN configuration interface.
2. Select "Port Based VLAN" at the VLAN Operation Mode, to enable the port-based VLAN function.
3. Click "Add" to create a new VLAN group. Then the following Figure 4-4-3 appears.
4. Type a name and Group ID for the new VLAN, the available range is 2-4094.
5. From the Available ports box, select ports to add to the IP DSLAM and click "Add".
6. Click Apply.
7. You will see the VLAN Group displays.
8. If the port-based VLAN groups list over one page, please click "Next Page" to view other VLAN groups on other page.
9. Use "Delete" button to delete unwanted port-based VLAN groups
10. Use "Edit" button to modify existing port-based VLAN groups.

By adding ports to the VLAN you have created one port-based VLAN group completely.

Figure 4-4-3: Static VLAN interface

The page includes the following fields:

Object	Description
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
Group ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094 .
Port	Indicate port 1 to port 10.
Member	Add Defines the interface as a Port-Based member of a VLAN.
	Remove Forbidden ports are not included in the VLAN.



All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

4.4.4 802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different DSLAM vendors. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create and delete Tag-based VLAN. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the IP DSLAM belong to default VLAN, VID is 1. The default VLAN can't be deleting.

Understand nomenclature of the IP DSLAM

■ IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant DSLAM can be configured as tagged or untagged.

- **Tagged** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the IP DSLAM). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

4.4.4.1 VLAN Group Configuration

■ VLAN Group Configuration

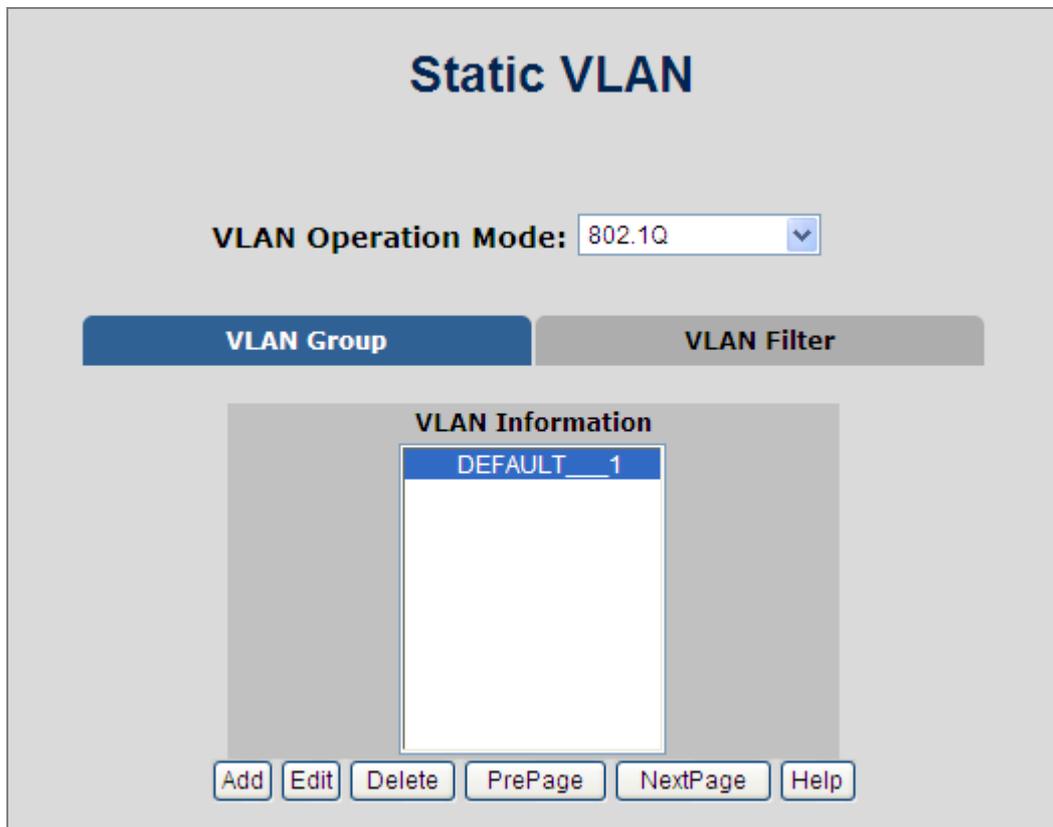


Figure 4-4-4: VLAN Group Configuration interface

1. Click the hyperlink "VLAN" \ "Static VLAN" to enter the VLAN configuration interface.
2. Select "802.1Q" at the **VLAN Operation Mode**, to enable the 802.1Q VLAN function.
3. Click **Add** to create a new VLAN group or Edit to management exist VLAN groups. Then the VLAN Group column appears.
4. Input a VLAN group ID and available range is 2-4094.

Static VLAN

VLAN Operation Mode: 802.1Q ▼

VLAN Group
VLAN Filter

VLAN Name:	<input style="width: 90%;" type="text"/>
VID:	<input style="width: 90%;" type="text" value="1"/>
<div style="border: 1px solid #ccc; padding: 2px;"> Port1 ▲ Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10 Port11 Port12 ▼ </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <input type="button" value="Add >>"/> <input type="button" value="<< Remove"/> </div>
<input type="checkbox"/> CPU Port	

Figure 4-4-5: VLAN Group Configuration interface

5. Select specific port as member port and the screen in Figure 4-4-6 appears.
6. After setup completed, please press "**Apply**" button to take effect.
7. Please press "**Back**" for return to VLAN configuration screen to add other VLAN group, the screen in Figure 4-33 appears.
8. If there are many groups that over the limit of one page, you can click "**Next**" to view other VLAN groups.
9. Use **Delete** button to delete unwanted VLAN.
10. Use **Edit** button to modify existing VLAN group.

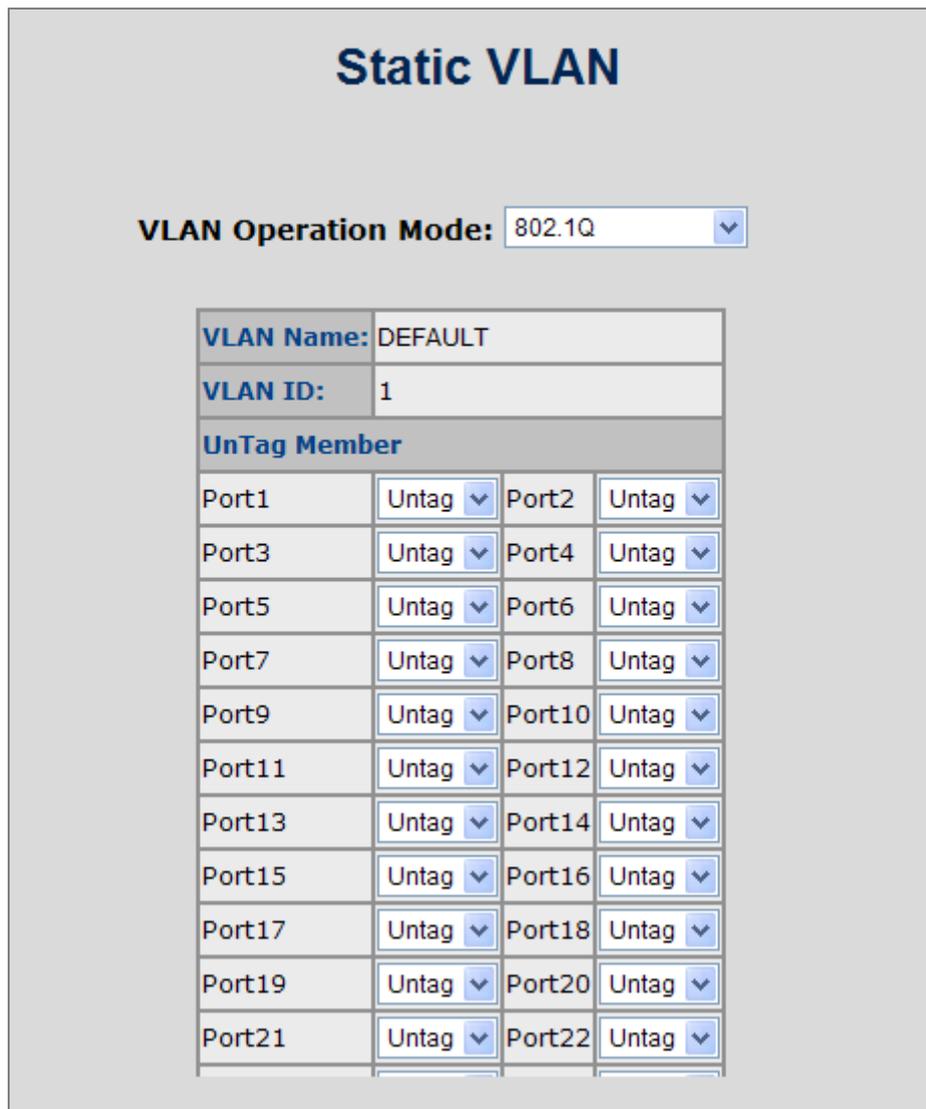


Figure 4-4-6: 802.1Q VLAN Setting Web Page screen

The page includes the following fields:

Object	Description
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
VLAN ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094 .
Port	Indicate port 1 to port 10.
UnTag Member	Untag Packets forwarded by the interface are untagged.
	Tag Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.



Enable 802.1Q VLAN, the all ports on the IP DSLAM belong to default VLAN, VID is 1. The default VLAN can't be deleted.

4.4.4.2 VLAN Filter

■ 802.1Q VLAN Port Configuration

This page is used for configuring the IP DSLAM port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (**PVID**) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

This section provides 802.1Q Ingress Filter of each port from the IP DSLAM, the screen in [Figure 4-4-7](#) appears.

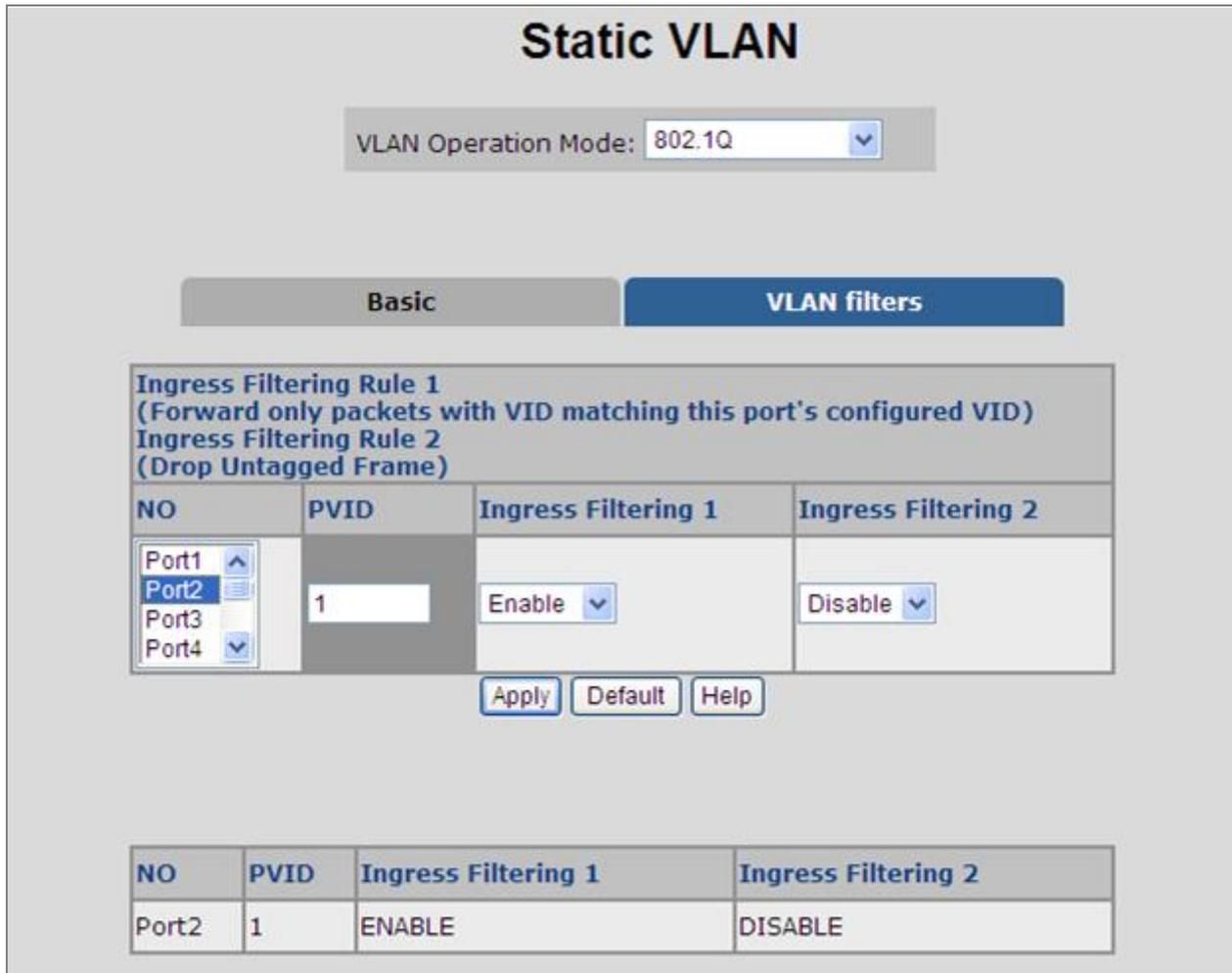


Figure 4-4-7: 802.1Q Ingress filter interface

The page includes the following fields:

Object	Description
NO	Indicate port 1 to port 10.
PVID	Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. The IP DSLAM each port allows user to set one VLAN ID, the range is 1~255,

	default VLAN ID is 1.
	The VLAN ID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.
Ingress Filtering 1	<p>Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.</p> <p>Enable: Forward only packets with VID matching this port's configured VID.</p> <p>Disable: Disable Ingress filter function.</p>
Ingress Filtering 2	<p>Drop untagged frame.</p> <p>Disable: Acceptable all Packet.</p> <p>Enable: Only packet with match VLAN ID can be permission to go through the port.</p>
Apply button	Press the button to save configurations.

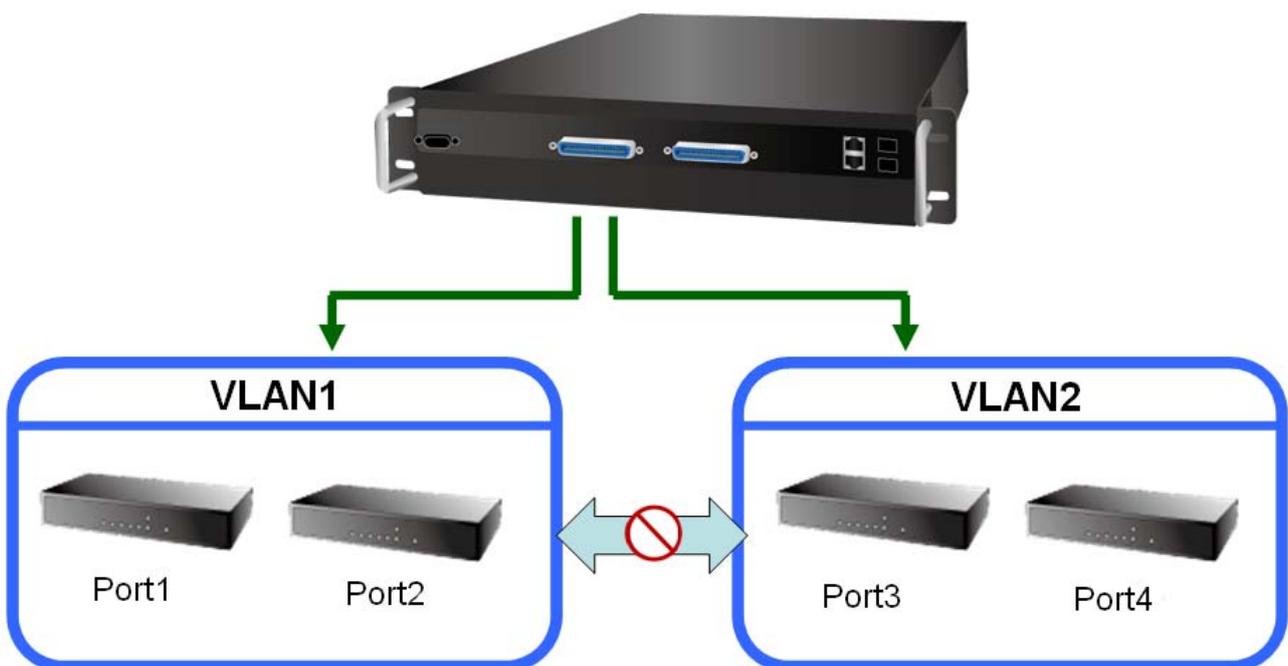
4.4.4.3 IEEE 802.1Q Symmetric VLAN Configuration Example

This section describes how to configure 802.1Q Symmetric VLAN on VDL-2420MR.

[Purpose]

Create 2 VLANs and the devices in the VLAN1 and VLAN2 can not access to each other.

[Topology]

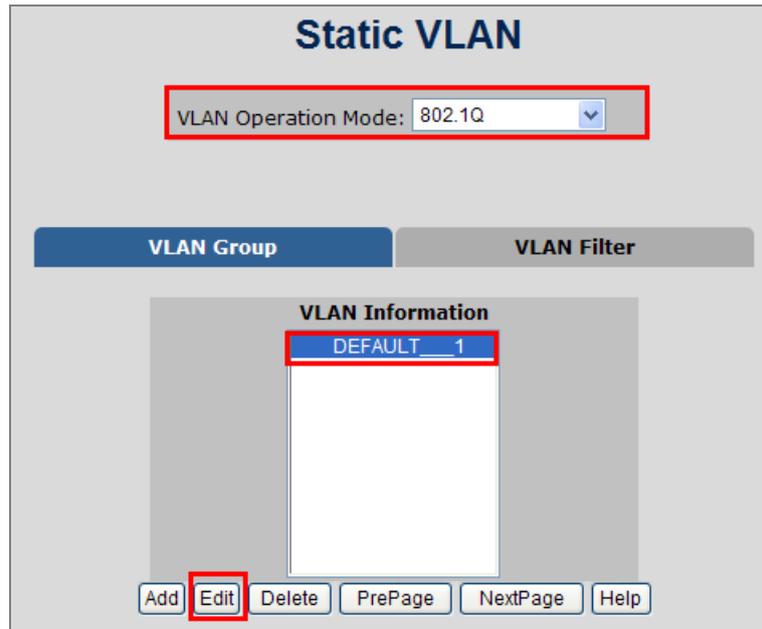




VLAN1 is system default value, so we configure VLAN2 and set VLAN1 and VLAN2 member can not access to each other.

[Procedure]

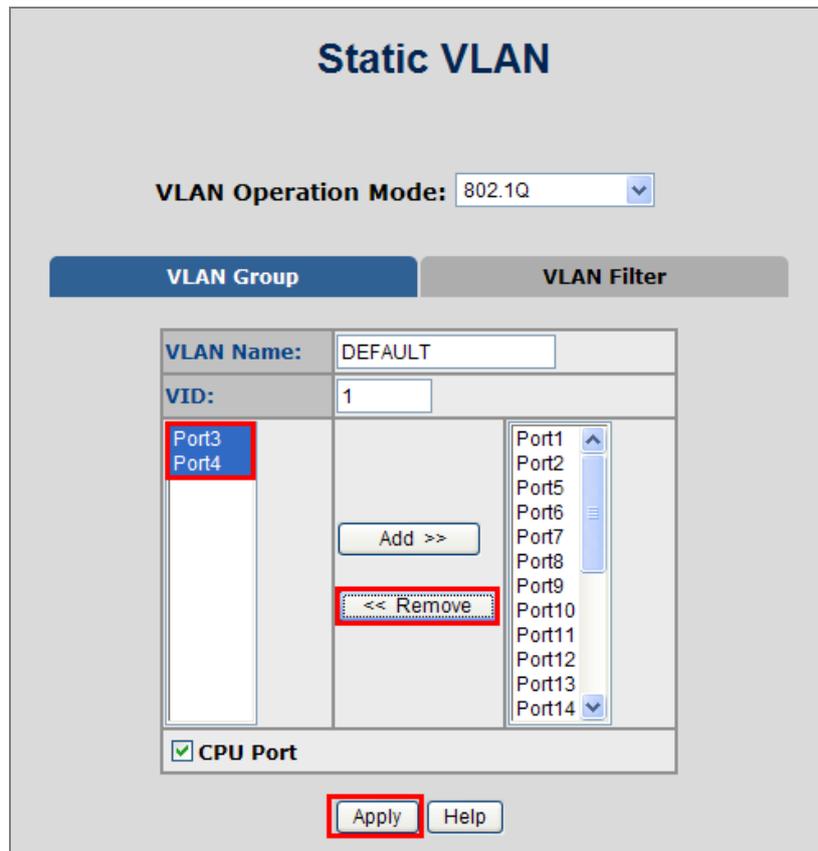
Step1. Make sure VLAN Operation Mode was selected to 802.1Q, then press **Edit** button to edit DEFAULT_1.



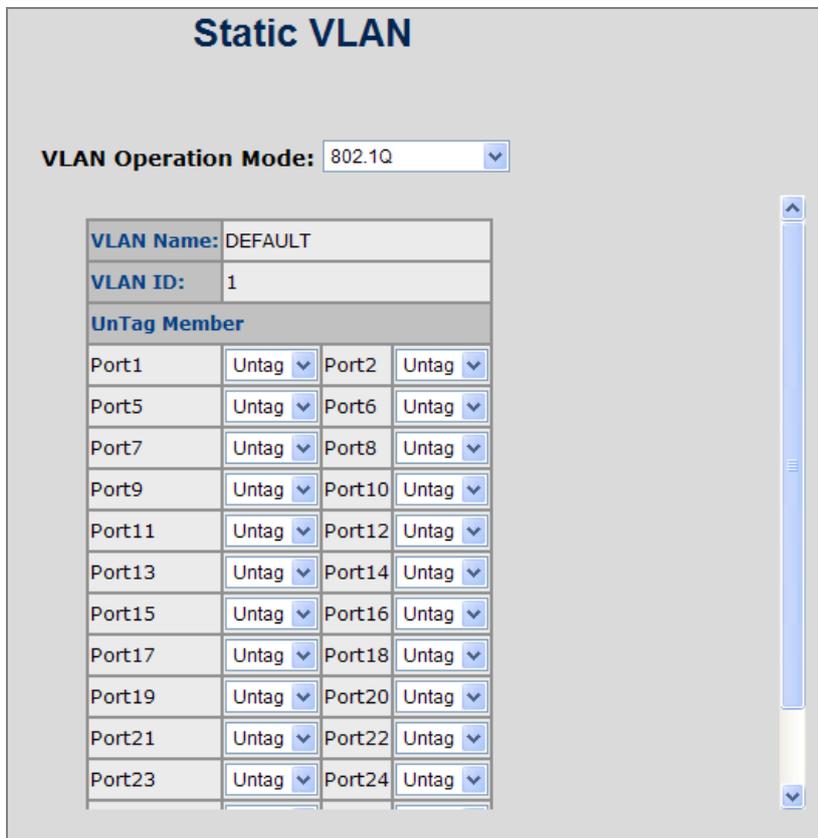
Step2. Select Port3 and Port4 from VLAN1 then press **Remove** button to remove it then press **Apply** button.



Why need to remove ports from VLAN1 when we want to assign the ports to another VLAN?
Because of we don't want make overlapping port.



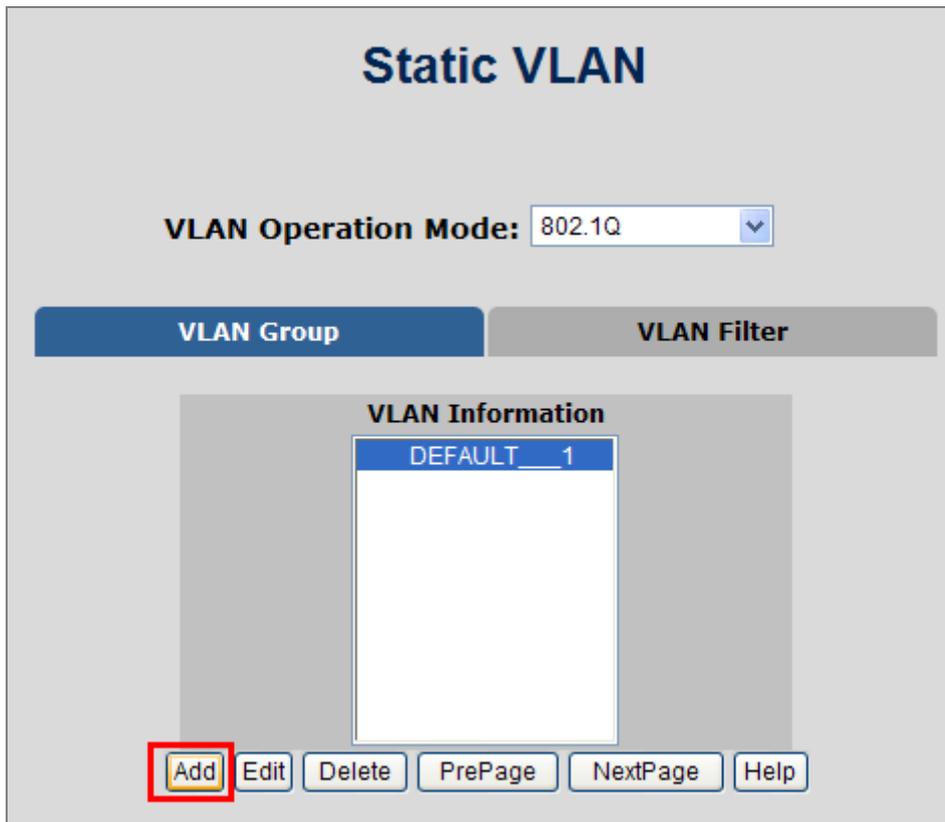
Step3. We don't need set any port to be Tag port, so please move scroll bar to bottom then press **Apply** button.



Step4. After Setp3, system will back to VLAN configure page and pop up a warning message window. This message window just figures out one or more ports have not been used in any VLAN. It is normal because we just removed port3 and port4 from default VLAN. Please press ok button to continue configuration.



Please Press **Add** button to create VLAN2 Group.



Step5. Please select port3 and port4 then press **Add** button to assign 2 ports to be VLAN2 member then press **Apply** button.



CPU Port features administrator could manage Switch via this VLAN. In default value this option is blank and not permit user manages Switch.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

VLAN Name:	VLAN2	
VID:	2	
<div style="border: 1px solid gray; padding: 2px;"> Port1 Port2 Port5 Port6 Port7 Port8 Port9 Port10 Port11 Port12 Port13 Port14 </div>	<div style="border: 1px solid gray; padding: 5px; display: inline-block;">Add >></div> <div style="border: 1px solid gray; padding: 5px; display: inline-block;"><< Remove</div>	<div style="border: 1px solid gray; padding: 2px;"> Port3 Port4 </div>
<input type="checkbox"/> CPU Port		

Apply
Help

Step6. Please select all ports to **Untag** then press **Apply** button. Now, system will back to VLAN configuration page.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Name:	VLAN2	
VLAN ID:	2	
Tag Member		
Port3	<div style="border: 1px solid red; padding: 2px;">Untag</div>	Port4
	<div style="border: 1px solid red; padding: 2px;">Untag</div>	

Apply

Step7. Now, we have to set up Port VLAN ID (PVID). Please click **VLAN Filter** then select Port3 and Port4 at **NO** field and change PVID form 1 to 2 then press **Apply** button.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1			
Port2			
Port3	2	Enable	Disable
Port4			

Apply
Default
Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port3	2	ENABLE	DISABLE
Port4	2	ENABLE	DISABLE

[END]

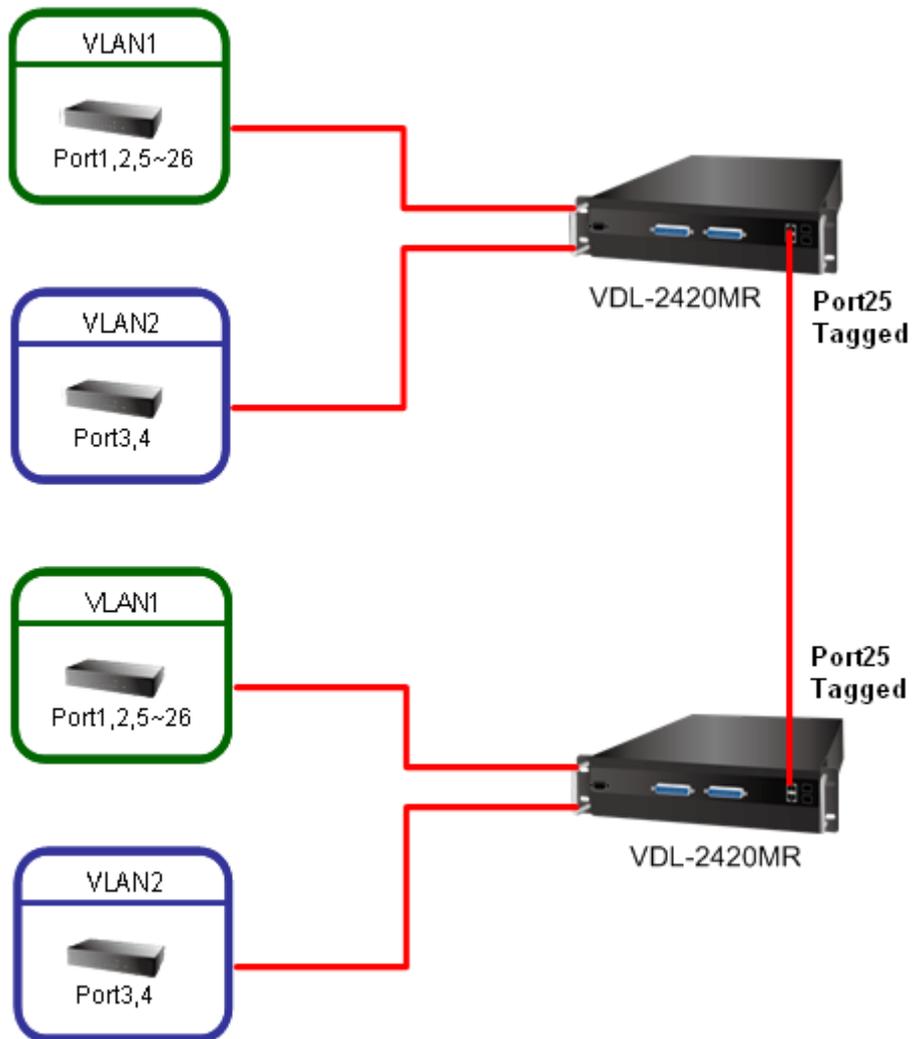
4.4.4.4 IEEE 802.1Q VLAN Trunk Configuration Example

This section describes how to configure 802.1Q VLAN Trunk on VDL-2420MR.

[Purpose]

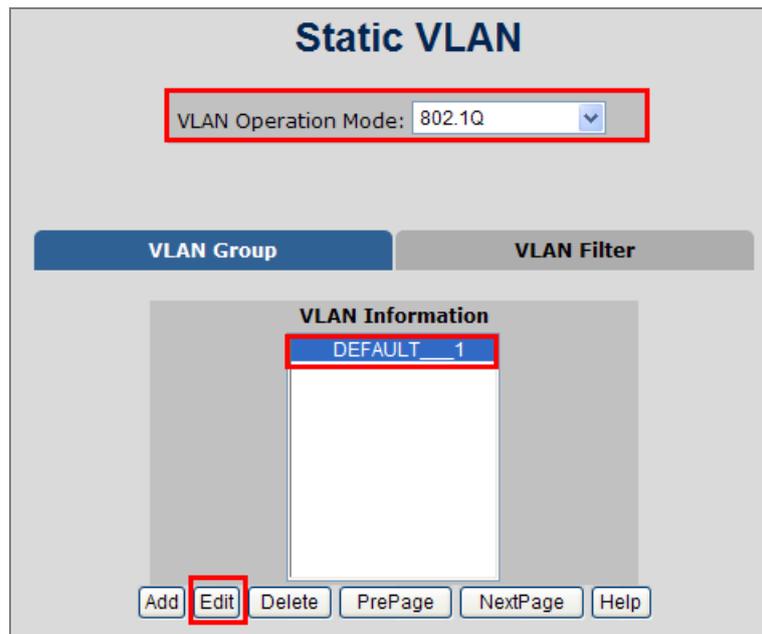
Create 2 VLANs on the 2 VDL-2420MR and the devices in the VLAN1 and VLAN2 can access to the other devices which stay on another VDL-2420MR VLAN1 and VLAN2 member. Also, VLAN1 and VLAN2 can not access to each other. VLANs can go through the Port25 Tagged port uplink to another VDL-2420MR or the Switch.

[Topology]



[Procedure]

Step1. Make sure VLAN Operation Mode was selected to 802.1Q, then press **Edit** button to edit DEFAULT_1.



Step2. Select Port3 and Port4 from VLAN1 then press **Remove** button to remove it then press **Apply** button.



Why need to remove ports from VLAN1 when we want to assign the ports to another VLAN?
Because of we don't want make overlapping port.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

VLAN Name:

VID:

Port3

Port4

Add >>

<< Remove

Port1

Port2

Port5

Port6

Port7

Port8

Port9

Port10

Port11

Port12

Port13

Port14

CPU Port

Apply Help

Step3. Please set port 25 to be Tag port, so that it could be uplink to another device then please press **Apply** button.

Static VLAN

VLAN Operation Mode: 802.1Q

UnTag Member

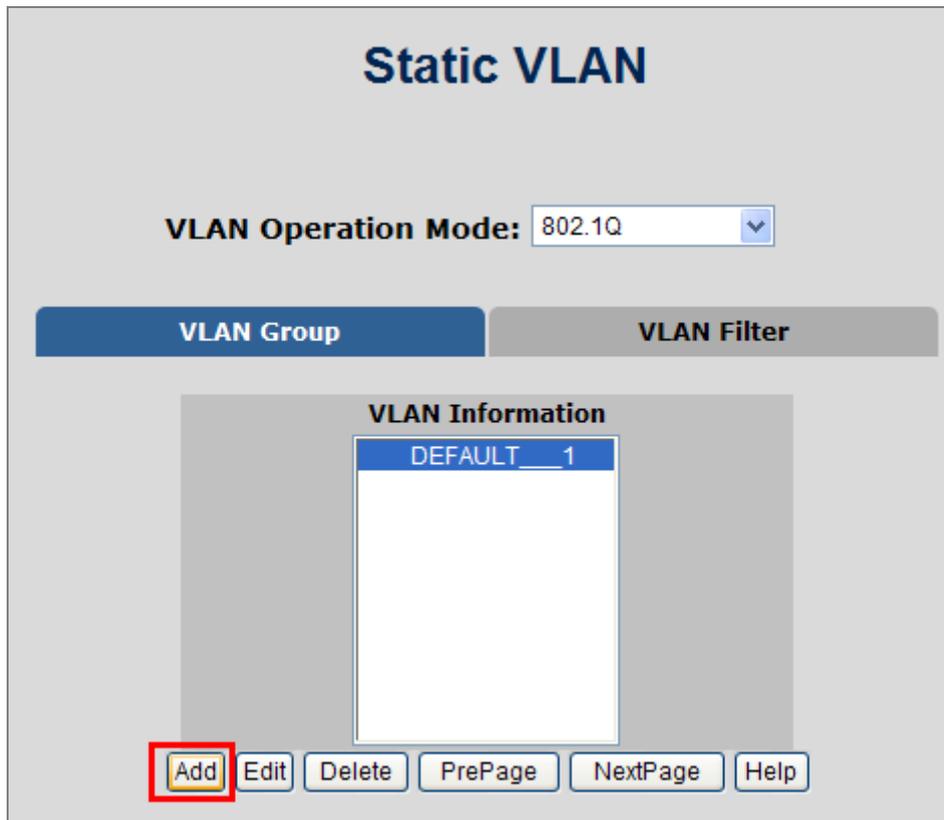
Port1	Untag	Port2	Untag
Port5	Untag	Port6	Untag
Port7	Untag	Port8	Untag
Port9	Untag	Port10	Untag
Port11	Untag	Port12	Untag
Port13	Untag	Port14	Untag
Port15	Untag	Port16	Untag
Port17	Untag	Port18	Untag
Port19	Untag	Port20	Untag
Port21	Untag	Port22	Untag
Port23	Untag	Port24	Untag
Port25	Tag	Port26	Untag

Apply

Step4. After Setp3, system will back to VLAN configure page and pop up a warning message window. This message window just figures out one or more ports have not been used in any VLAN. It is normal because we just removed port3 and port4 from default VLAN. Please press ok button to continue configuration.



Please Press **Add** button to create VLAN2 Group.



Step5. Please select port3, port4 and port25 then press **Add** button to assign 3 ports to be VLAN2 member then press **Apply** button.



CPU Port features administrator could manage Switch via this VLAN. In default value this option is blank and not permit user manages Switch.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

VLAN Name:	VLAN2	
VID:	2	
<div style="border: 1px solid gray; padding: 2px;"> Port14 ▲ Port15 Port16 Port17 Port18 Port19 Port20 Port21 Port22 Port23 Port24 Port26 ▼ </div>	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Add >></div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"><< Remove</div>	<div style="border: 1px solid gray; padding: 2px;"> Port3 Port4 Port25 </div>
<input type="checkbox"/> CPU Port		

Step6. Please select all ports to **Untag** but port 25 then press **Apply** button. Now, system will back to VLAN configuration page.

VLAN Operation Mode: 802.1Q

VLAN Name:	VLAN2	
VLAN ID:	2	
Tag Member		
Port3	Untag ▼	Port4 Untag ▼
Port25	Tag ▼	

Step7. Now, we have to set up Port VLAN ID (PVID). Please click **VLAN Filter** then select Port3 and Port4 at **NO** field and change PVID form 1 to 2 then press **Apply** button.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1			
Port2			
Port3	2	Enable	Disable
Port4			

Apply
Default
Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port3	2	ENABLE	DISABLE
Port4	2	ENABLE	DISABLE

Step8. Do the same configuration on another one VDL-2420MR.

Step9. Connect port 25 to port 25, just like as topology.

[END]

4.4.4.5 IEEE 802.1Q Overlapping VLAN Configuration Example

This section describes how to configure 802.1Q overlapping VLAN on VDL-2420MR.
 The overlapping feature usually applies to access specified port from specified VLAN.



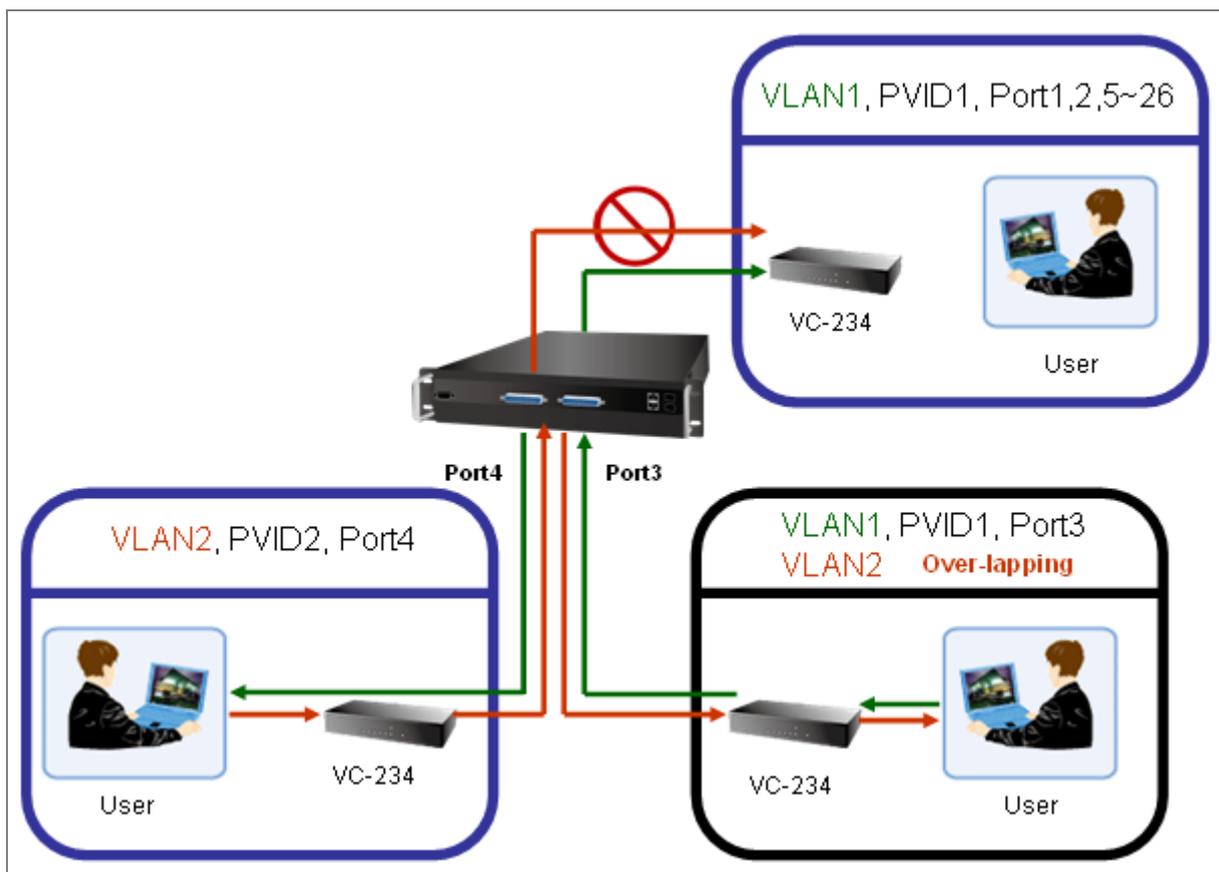
Note

Sometimes the Overlapping VLAN means Asymmetric VLAN.

[Purpose]

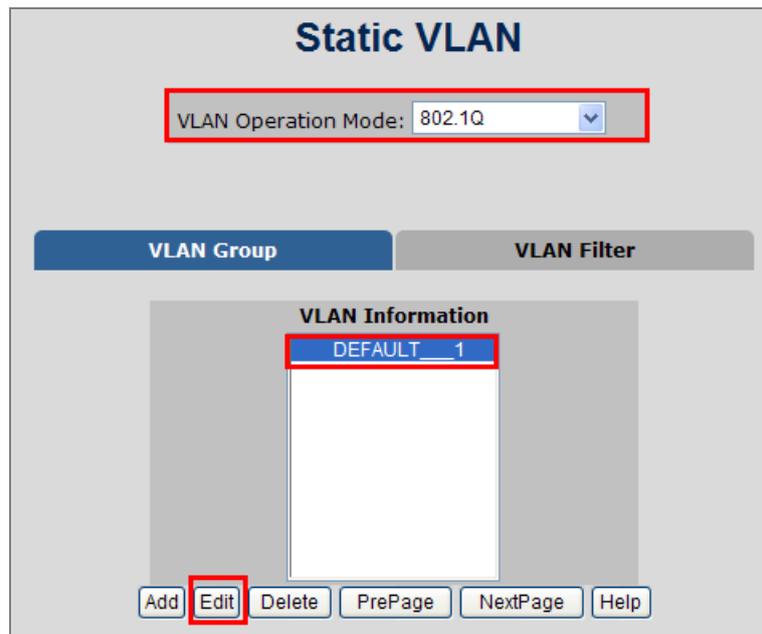
Create 2 VLANs on the VDL-2420MR and we specify port3 can be VLAN2 member port access and also port3 can be accessed by VLAN1 member port. Because of port3 can be accessed from VLAN1 and VLAN2 member port, so port3 is an overlapping port.

[Topology]

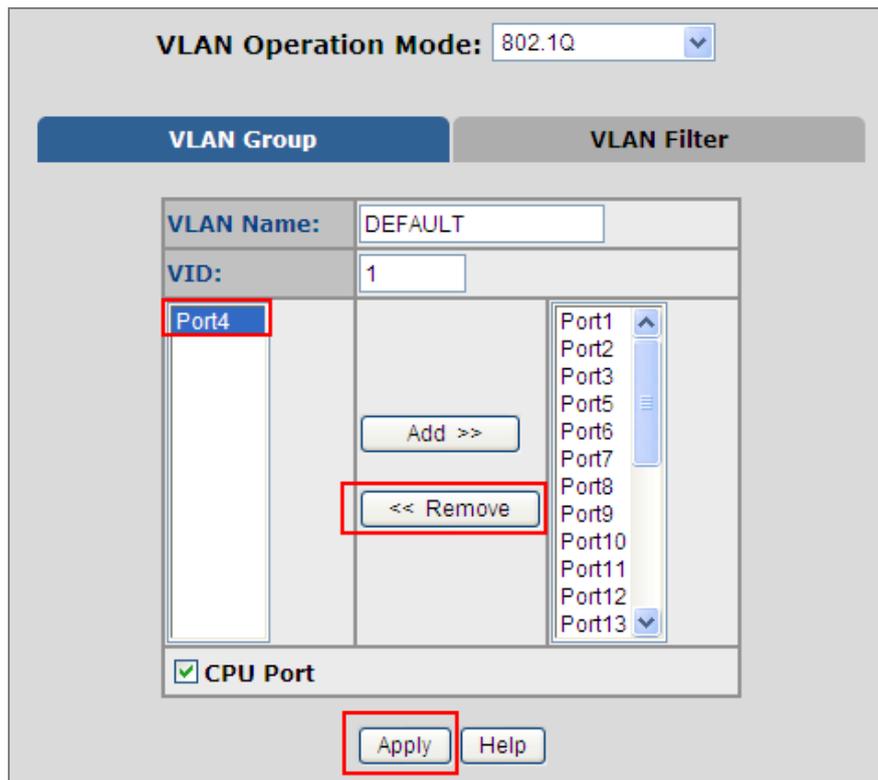


[Procedure]

Step1. Make sure VLAN Operation Mode was selected to 802.1Q, then press **Edit** button to edit DEFAULT_1.



Step2. Remove Port4 from VLAN1 then press **Apply** button.



Step3. Keep all port to Untag and press **Apply** button.

VLAN Operation Mode: 802.1Q

Port1	Untag	Port2	Untag
Port3	Untag	Port5	Untag
Port6	Untag	Port7	Untag
Port8	Untag	Port9	Untag
Port10	Untag	Port11	Untag
Port12	Untag	Port13	Untag
Port14	Untag	Port15	Untag
Port16	Untag	Port17	Untag
Port18	Untag	Port19	Untag
Port20	Untag	Port21	Untag
Port22	Untag	Port23	Untag
Port24	Untag	Port25	Untag
Port26	Untag		

Apply

Step4. Press **Add** button to add VLAN2 group.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

VLAN Information

DEFAULT__1

Add | Edit | Delete | PrePage | NextPage | Help

Step5. Add Port3 and Port4 to be VLAN2 group member.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

VLAN Name: VLAN2

VID: 2

Port1
Port2
Port5
Port6
Port7
Port8
Port9
Port10
Port11
Port12
Port13
Port14

Port3
Port4

Add >>

<< Remove

CPU Port

Apply Help

Step6. Please select all ports to **Untag** then press **Apply** button. Now, system will back to VLAN configuration page.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Name: VLAN2

VLAN ID: 2

Tag Member

Port3 Untag Port4 Untag

Apply

Step7. Click VLAN Filter page and select Port4 then input PVID to 2 then press **Apply** button.

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1			
Port2			
Port3			
Port4	2	Enable	Disable

Apply | Default | Help

Step8. Check Port3 and Port4 PVID status.

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1			
Port2			
Port3	1	Enable	Disable
Port4			

Apply | Default | Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port3	1	ENABLE	DISABLE
Port4	2	ENABLE	DISABLE

[END]

4.4.4.6 Port Trunk + IEEE 802.1Q VLAN Trunk Configuration Example

This section describes how to configure Port Trunk work on the 802.1Q VLAN Trunk on VDL-2420MR.

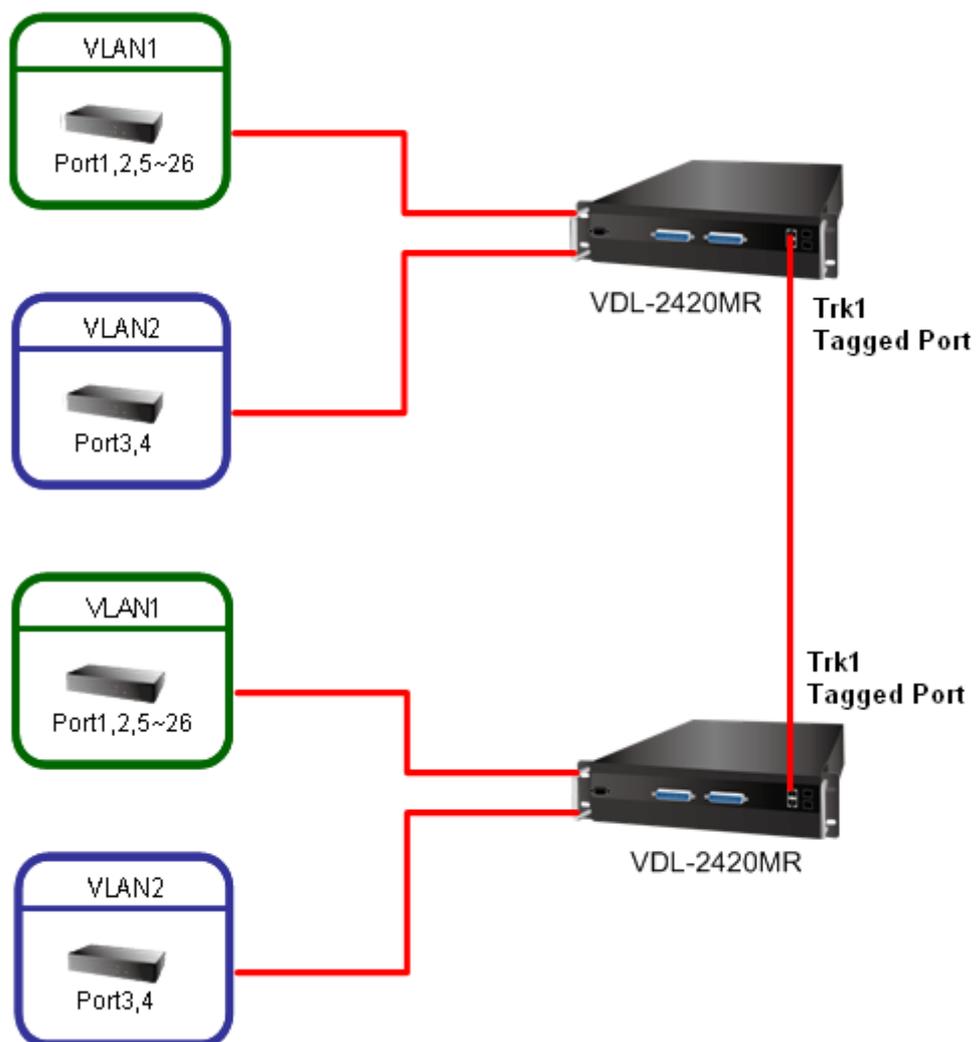
[Purpose]

Configure Port25 and Port 26 to be LACP port trunk named **Trk1**.

Create 2 VLANs on the 2 VDL-2420MR and the CPE devices in the VLAN1 and VLAN2 can access to the other devices which stay on another VDL-2420MR VLAN1 and VLAN2 member **via a LACP port trunk**. Also, VLAN1 and VLAN2 can not access to each other.

VLANs can go through the **Trk1** Tagged port uplink to another VDL-2420MR or the Switch.

[Topology]

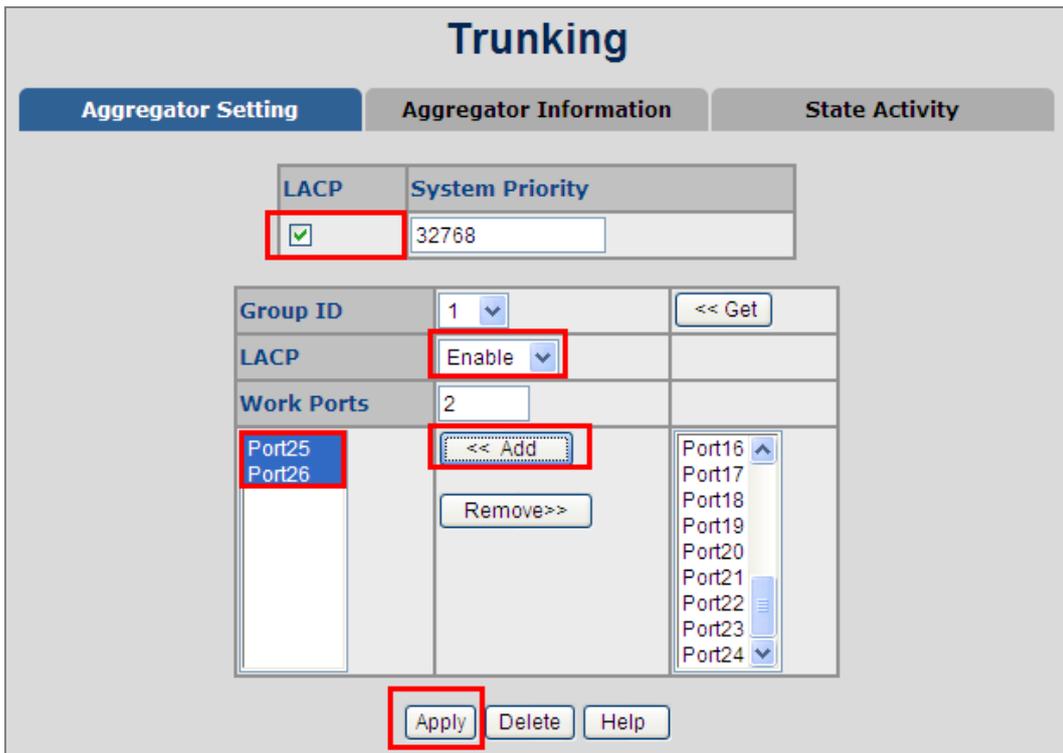


[Procedure]

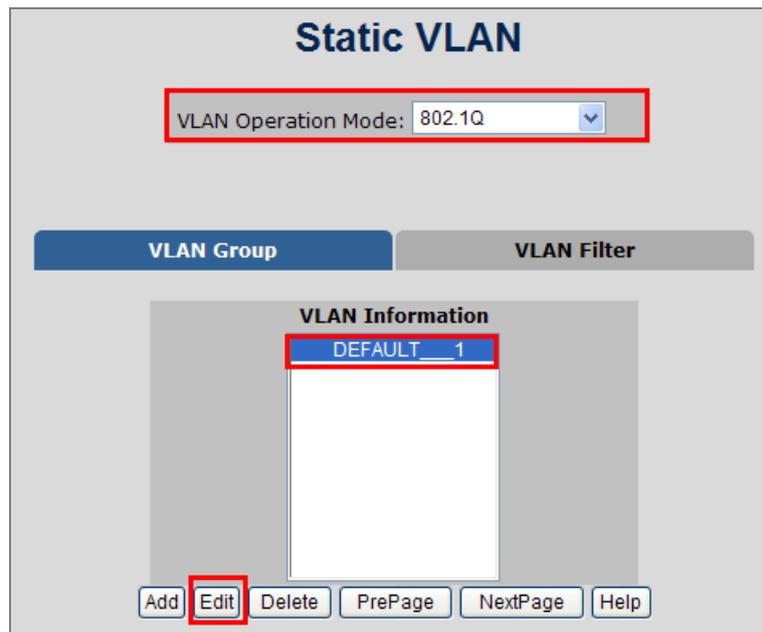
Step1. Click Trunking option on the Menu.



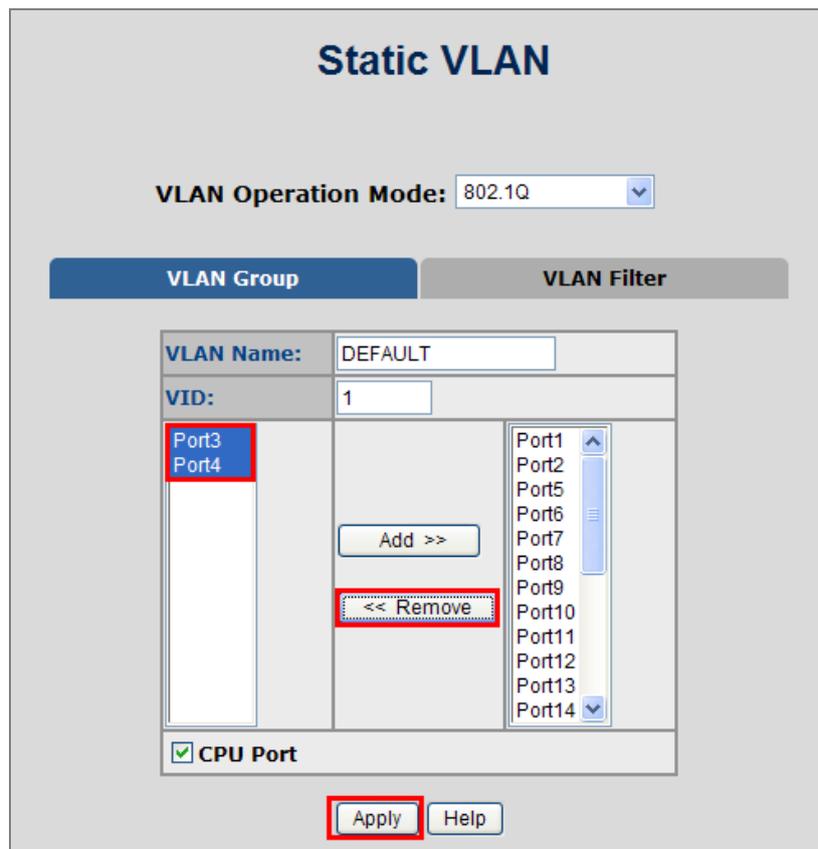
Step2. Select LACP option and enable LACP then add Port25 and Port26 then press **Apply** button then we can get **Trk1**.



Step3. Make sure VLAN Operation Mode was selected to 802.1Q, then press **Edit** button to edit DEFAULT_1.



Step4. Remove Port3 and Port4 from VLAN1 then press Apply button.



Step5. Select **Trk1** to Tag then press Apply button.

The screenshot shows the 'VLAN Operation Mode' set to '802.1Q'. Below this is a table titled 'UnTag Member' with 24 rows and 2 columns. Each row contains a port number (Port1 to Port24) and a dropdown menu currently set to 'Untag'. The 'Trk1' label and its corresponding 'Tag' dropdown menu are highlighted with a red box. Below the table, the 'Apply' button is also highlighted with a red box.

UnTag Member	
Port1	Untag
Port2	Untag
Port5	Untag
Port6	Untag
Port7	Untag
Port8	Untag
Port9	Untag
Port10	Untag
Port11	Untag
Port12	Untag
Port13	Untag
Port14	Untag
Port15	Untag
Port16	Untag
Port17	Untag
Port18	Untag
Port19	Untag
Port20	Untag
Port21	Untag
Port22	Untag
Port23	Untag
Port24	Untag
Trk1	Tag

Apply

Step6. Please Press **Add** button to create VLAN2 Group.

The screenshot shows the 'Static VLAN' configuration page. At the top, 'VLAN Operation Mode' is set to '802.1Q'. Below this are two tabs: 'VLAN Group' (active) and 'VLAN Filter'. Under the 'VLAN Group' tab, there is a 'VLAN Information' section with a table containing one entry: 'DEFAULT__ 1'. At the bottom of the page, there is a row of buttons: 'Add', 'Edit', 'Delete', 'PrePage', 'NextPage', and 'Help'. The 'Add' button is highlighted with a red box.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group | VLAN Filter

VLAN Information

VLAN Information
DEFAULT__ 1

Add Edit Delete PrePage NextPage Help

Step7. Please select port3, port4 and port **Trk1** then press **Add** button to assign 3 ports to be VLAN2 member then press **Apply** button.



CPU Port features administrator could manage Switch via this VLAN. In default value this option is blank and not permit user manages Switch.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

VLAN Name:	VLAN2	
VID:	2	
<ul style="list-style-type: none"> Port14 Port15 Port16 Port17 Port18 Port19 Port20 Port21 Port22 Port23 Port24 Port26 	<div style="margin-bottom: 10px;">Add >></div> <div style="margin-bottom: 10px;"><< Remove</div>	<div style="border: 1px solid #0056b3; padding: 5px; background-color: #0056b3; color: white; margin-bottom: 10px;"> Port3 Port4 Trk1 </div>
<input type="checkbox"/> CPU Port		

Apply
Help

Step8. Please select all ports to **Untag** but port **Trk1** then press **Apply** button. Now, system will back to VLAN configuration page.

VLAN Operation Mode: 802.1Q

VLAN Name: VLAN2

VLAN ID: 2

Tag Member

Port3: Untag Port4: Untag

Trk1: Tag

Apply

Step9. Now, we have to set up Port VLAN ID (PVID). Please click **VLAN Filter** then select Port3 and Port4 at **NO** field and change PVID form 1 to 2 then press **Apply** button.

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1			
Port2			
Port3	2	Enable	Disable
Port4			

Apply | Default | Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port3	2	ENABLE	DISABLE
Port4	2	ENABLE	DISABLE

Step8. Do the same configuration on another one VDL-2420MR.

Step9. Connect VDL-2420MR Port 25 and Port 26 to each other, just like as topology.

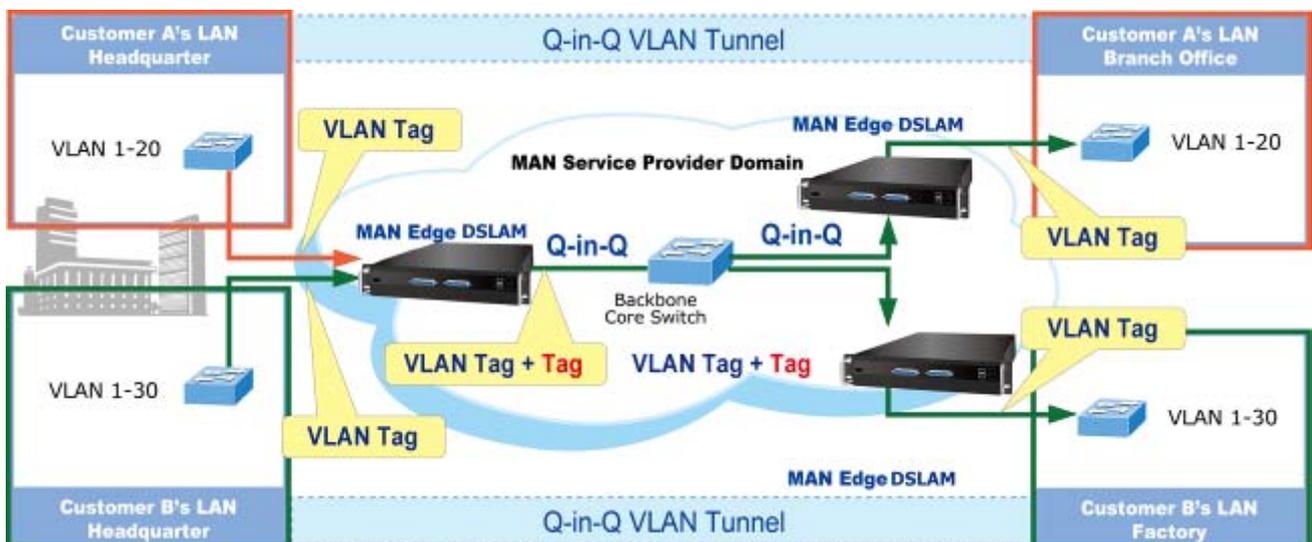
[END]

4.4.5 Q-in-Q VLAN

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The IP DSLAM supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use Ether Type **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the IP DSLAM, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

4.4.5.1 Q-in-Q Port Setting

The QinQ VLAN \ **QinQ Port Setting** screen in [Figure 4-4-8](#) appears.

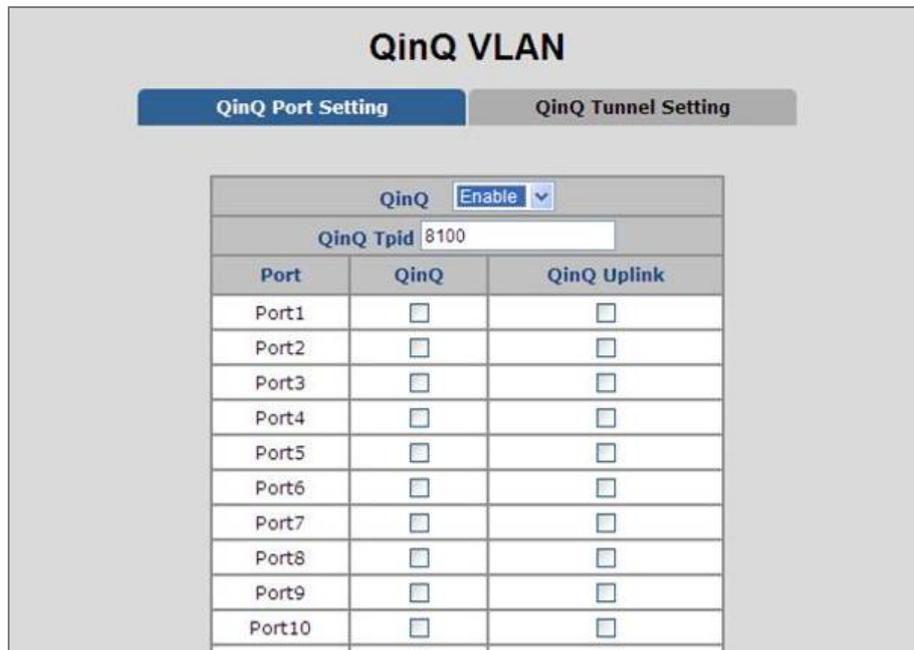


Figure 4-4-8: Q-in-Q Port Setting interface

The page includes the following fields:

Object	Description
QinQ	Enable: Sets the IP DSLAM to QinQ mode, and allows the QinQ tunnel port to be configured.
	Disable: The IP DSLAM operates in its normal VLAN mode.
QinQ TPID	The default is for the IP DSLAM to function in Disable mode.
	The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port. <ul style="list-style-type: none"> • 802.1Q Tag: 8100 • vMAN Tag: 88A8 Default: 802.1Q Tag.
Port QinQ	Check: Sets the Port to QinQ mode. Or the port operates in its normal VLAN mode.
	Default: Un-check.
QinQ Uplink	Check: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.
	Cancel: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

4.4.5.2 Q-in-Q Tunnel Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs.

Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

The screenshot shows the 'QinQ VLAN' configuration page with the 'QinQ Tunnel Setting' tab selected. The interface contains the following elements:

- Tunnel ID:** A dropdown menu currently showing 'Tunnel1'.
- Tunnel VID:** A text input field containing the value '0'.
- Port Selection:** A list of ports from Port1 to Port9. Port1 is currently selected.
- Buttons:** '<< Get' (to refresh the port list), '<< Add <<' (to add selected ports to the tunnel), and 'Remove >>' (to remove selected ports from the tunnel).
- Footer Buttons:** 'Apply', 'Delete', and 'Help'.

Figure 4-4-9: Q-in-Q Tunnel Setting interface

■ To configure QinQ Port

1. Enable global QinQ function: select **QinQ** enable "**Enable**".
2. Fill QinQ Tpid.
3. Enable port QinQ function: select QinQ checkbox for special port.
4. Enable port QinQ Uplink function: select QinQ Uplink checkbox for special port.

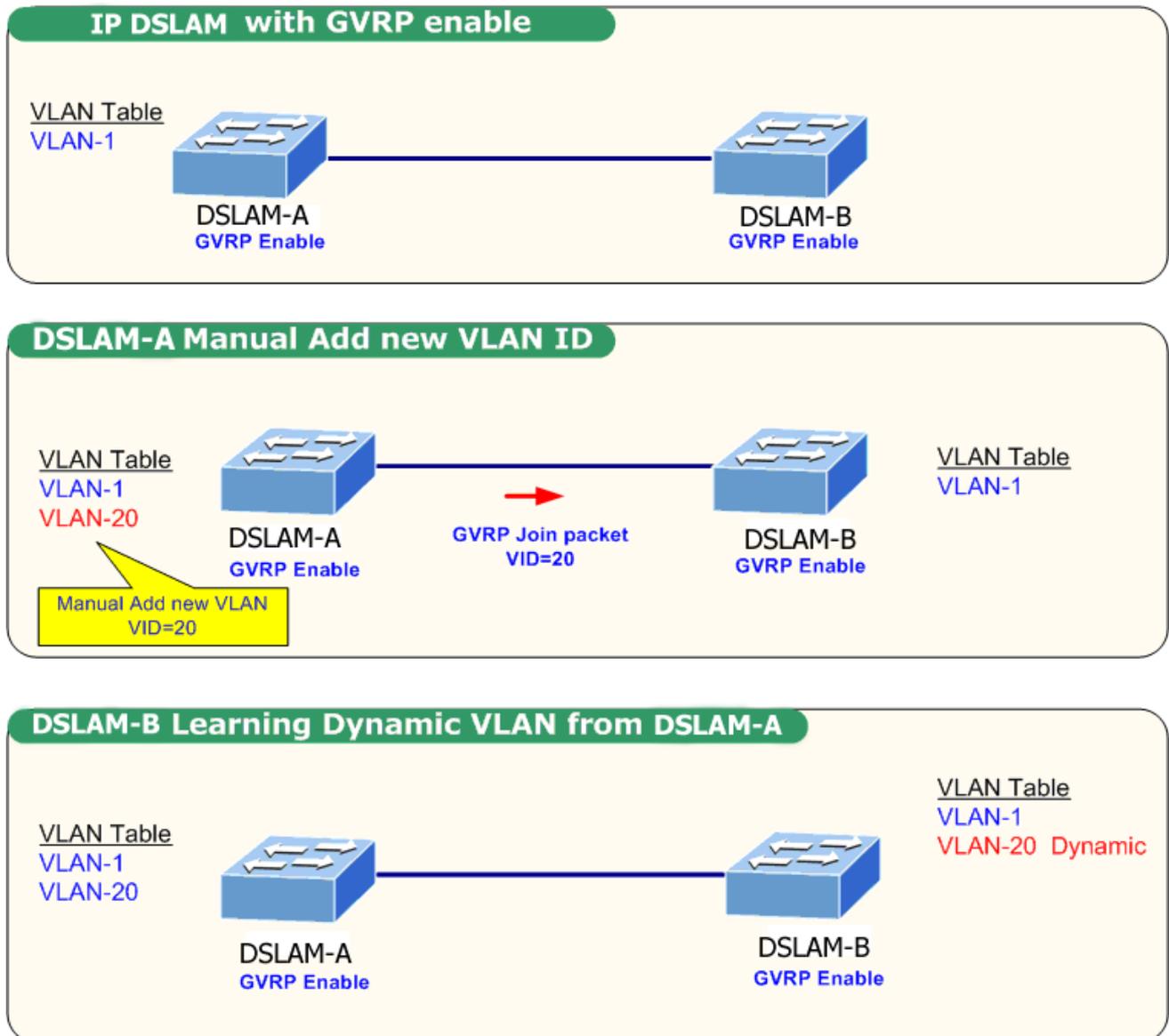


Note

Please make sure port has been remove from VLAN1 and not be used by any VLAN before configure Q-in-Q.

4.4.6 GVRP VLAN

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. Please refer to



4.4.6.1 GVRP Setting

To configure GVRP

Enable global GVRP function: select GVRP enable "Enable".

Enable port GVRP function: select GVRP checkbox for special port.

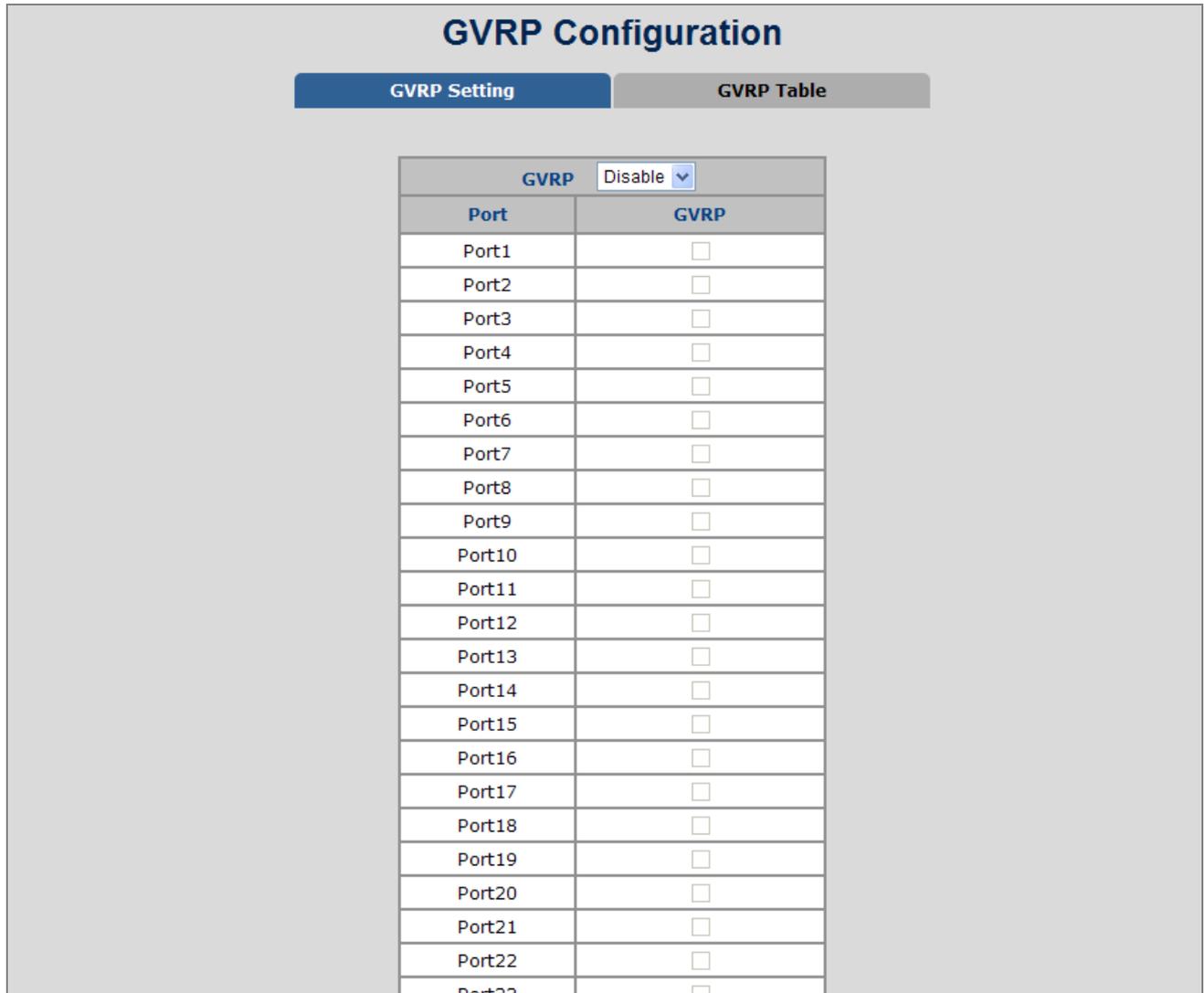


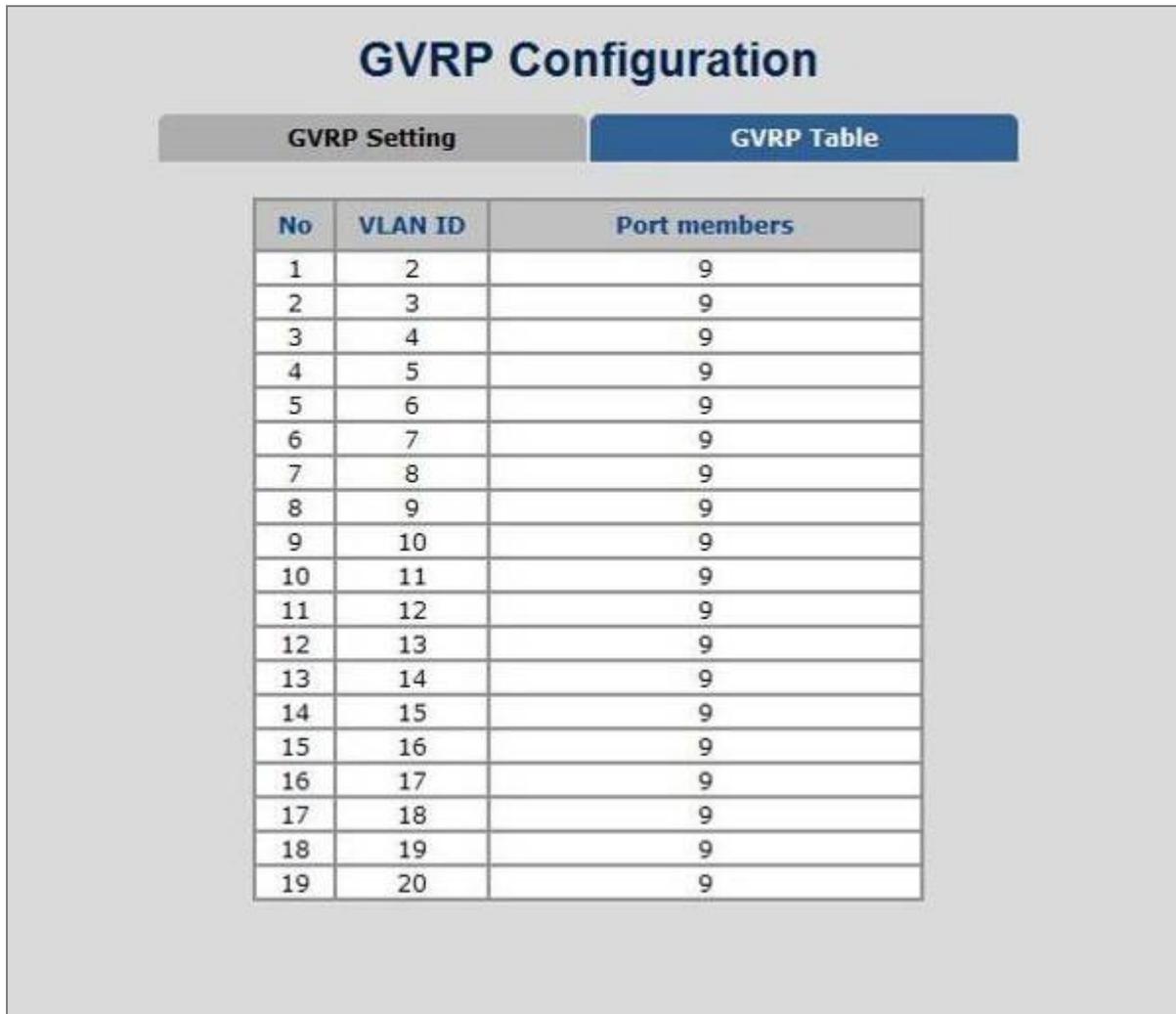
Figure 4-4-10: GVRP Configuration Web interface

The page includes the following fields:

Object	Description
GVRP	Enable global GVRP function
Port	Indicate port 1 to port 10.
Port GVRP	Enable selected port GVRP function

4.4.6.2 GVRP Table

The GVRP Table can be used to display dynamic VLANs from being learned via GVRP.



GVRP Configuration

GVRP Setting
GVRP Table

No	VLAN ID	Port members
1	2	9
2	3	9
3	4	9
4	5	9
5	6	9
6	7	9
7	8	9
8	9	9
9	10	9
10	11	9
11	12	9
12	13	9
13	14	9
14	15	9
15	16	9
16	17	9
17	18	9
18	19	9
19	20	9

Figure 4-4-11: GVRP Table Web interface

The page includes the following fields:

Object	Description
VLAN ID	Display the learned VLANs via GVRP protocol on GVRP enabled ports. The IP DSLAM allows displaying up to 128 dynamic VLAN entries.
Port Members	Identify the GVRP enabled port that dynamic VLAN is learned from.

4.5 Trunking

Port Trunking (also called “Link Aggregation”) is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. The IP DSLAM supports two types of port trunk technology:

- **Static Trunk**
- **LACP**

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires Full-duplex mode**, more detail information refers to IEEE 802.3ad.

4.5.1 Aggregator setting

This section provides Port Trunk-Aggregator Setting of each port from the IP DSLAM, the screen in [Figure 4-5-1](#) appears.

Figure 4-5-1: Port Trunk—Aggregator setting interface (two ports are added to the left field with LACP enabled)

The page includes the following fields:

Object	Description
System Priority:	A value which is used to identify the active LACP. The IP DSLAM with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.

Group ID:	There are 13 trunk groups to be selected. Assign the " Group ID " to the trunk group.
LACP:	<ul style="list-style-type: none"> ■ Enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. ■ Disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
Work ports:	This column field allows the user to type in the total number of active port up to four. With LACP static trunk group , e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group (non-LACP), the number of work ports must equal the total number of group member ports.



Please notice that a trunk group, including member ports split between two switches, **has to enable the LACP function of the two switches.**

4.5.2 Aggregator Information

When you had setup the LACP aggregator, you will see relation information in here.

■ LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.

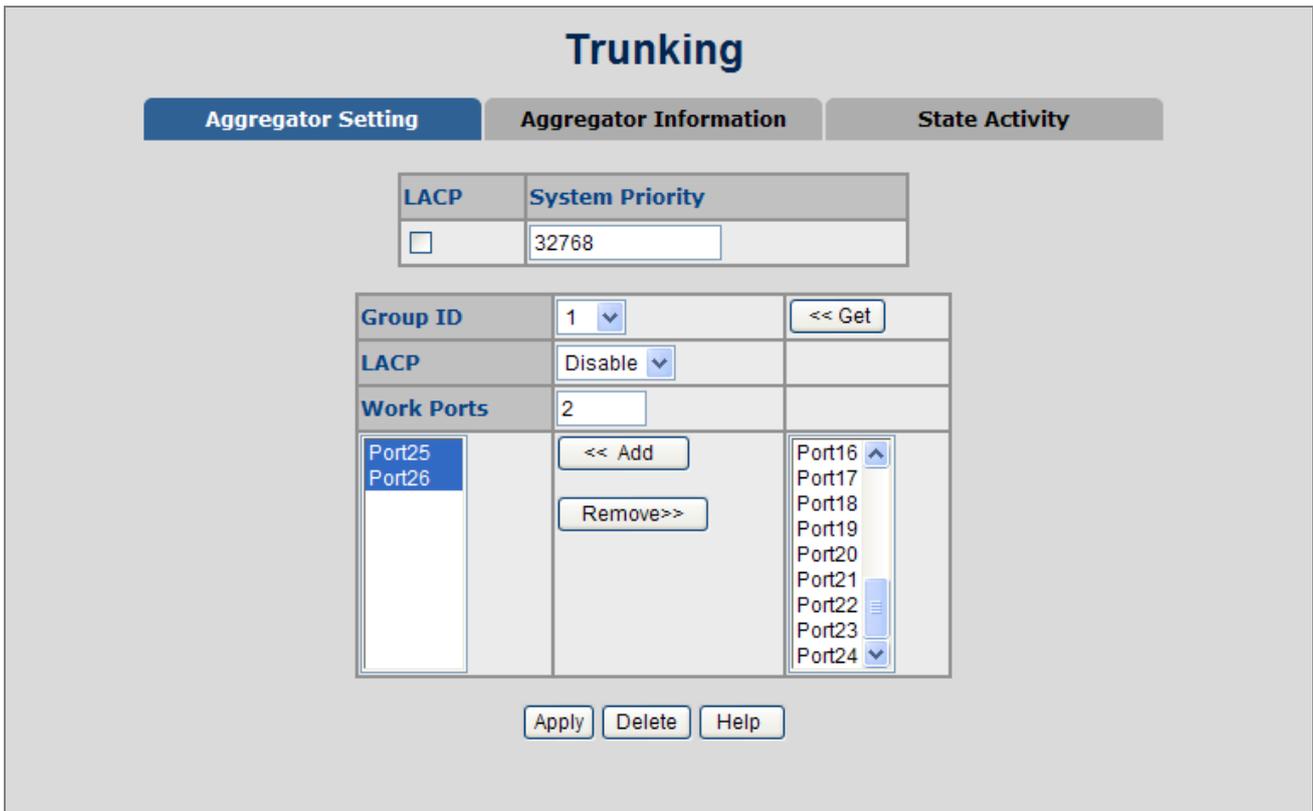


Figure 4-5-2: Assigning 2 ports to a trunk group with LACP disabled

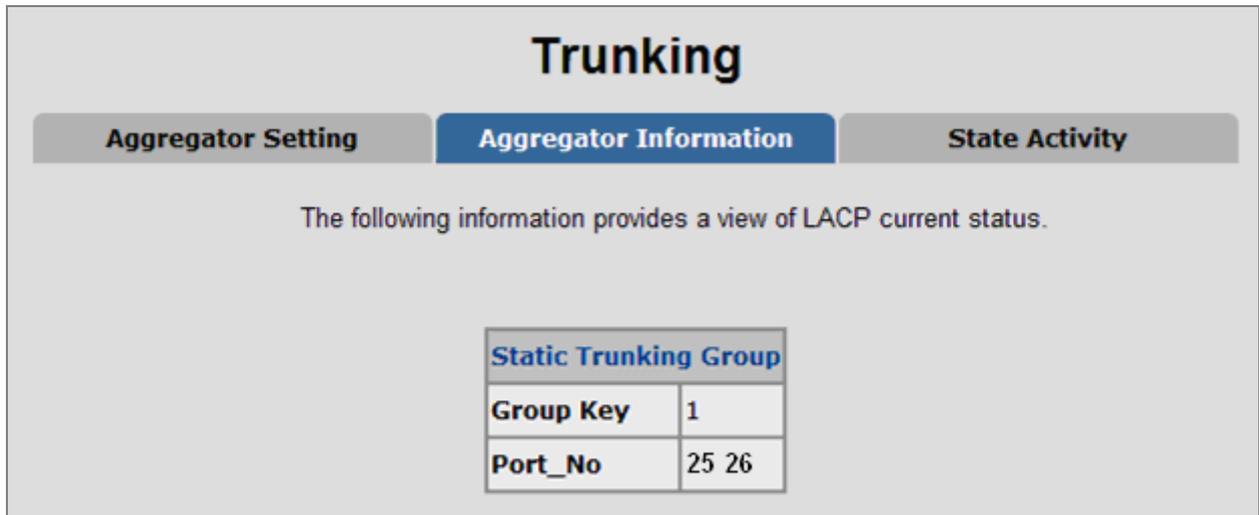


Figure 4-5-3: Static Trunking Group information

The page includes the following fields:

Object	Description
Group Key:	This is a read-only column field that displays the trunk group ID.
Port Member:	This is a read-only column field that displays the members of this static trunk group.

■ LACP enabled

Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

■ DSLAM1 configuration

1. Set **System Priority** of the trunk group. The default is **32768**.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable **LACP**.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

The screenshot shows the 'Trunking' configuration page with three tabs: 'Aggregator Setting', 'Aggregator Information', and 'State Activity'. The 'Aggregator Information' tab is active. It contains a table with 'LACP' (checked) and 'System Priority' (32768). Below this is a 'Group ID' dropdown set to '1' with a '<< Get' button. The 'LACP' dropdown is set to 'Disable'. The 'Work Ports' field is set to '2'. A 'Work Ports' column contains 'Port1' and 'Port2'. To the right is a list of ports from 'Port3' to 'Port11'. Below the list are '<< Add' and 'Remove>>' buttons. At the bottom are 'Apply', 'Delete', and 'Help' buttons.

Figure 4-5-4: Aggregation Information of **DSLAM 1**

5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

■ DSLAM2 configuration

6. Set **System Priority** of the trunk group. For example: 1.
7. Select a **trunk group ID** by pull down the drop-down menu bar.
8. Enable LACP.
9. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

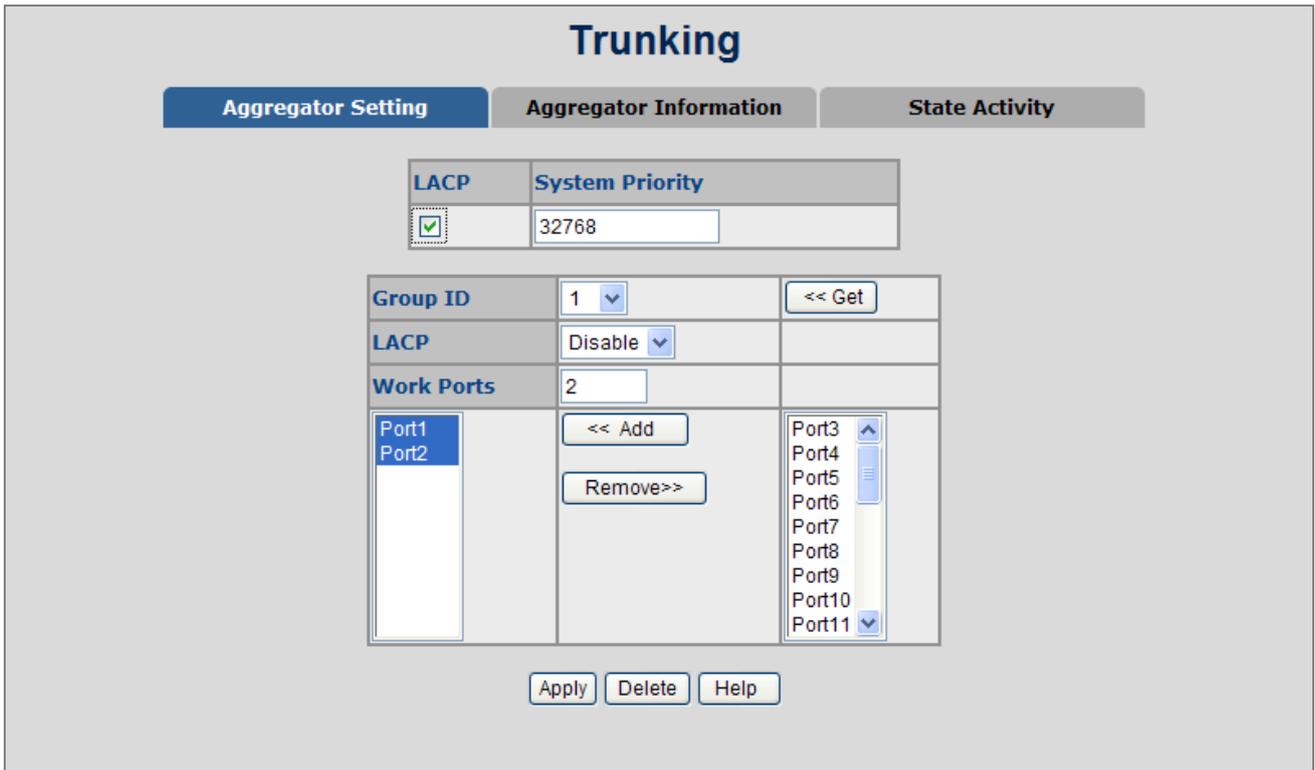


Figure 4-5-5: DSLAM 2 configuration interface

10. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.



Figure 4-5-6: DSLAM 1 Aggregator Information

4.5.3 State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click **Apply**, the port state activity will change to **Passive**.

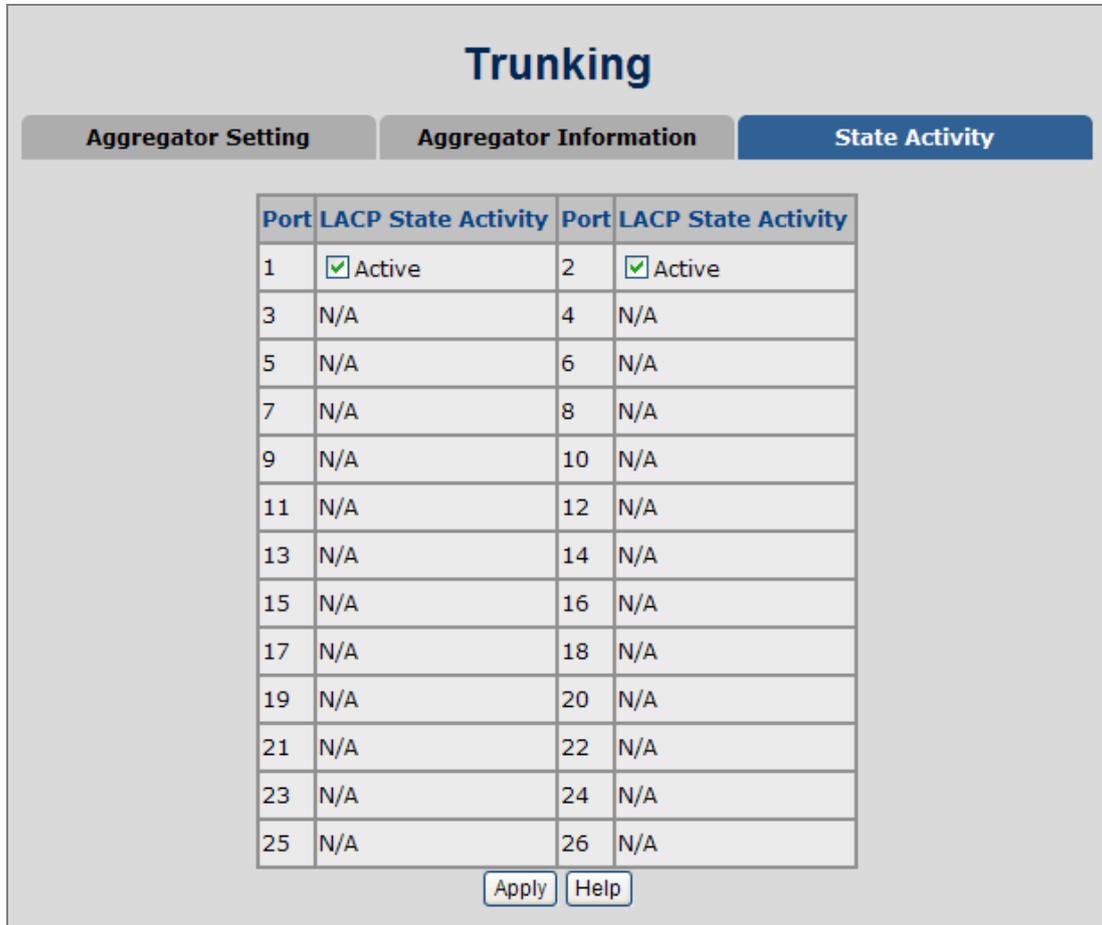


Figure 4-5-7: State Activity of DSLAM1

The page includes the following fields:

Object	Description
Active:	The port automatically sends LACP protocol packets.
Passive:	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.



A link having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

4.6 Forwarding and Filtering

The frames of Ethernet Packets contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the IP DSLAM to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

4.6.1 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The Dynamic MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. You can view all of the dynamic MAC addresses learned by the listed port.

The screenshot shows the 'Forwarding and Filtering' interface with the 'Dynamic MAC Table' tab selected. It includes a 'Clear' button and a table of dynamic MAC addresses.

NO	MAC	PORT	VID	TYPE
1	00:08:B6:00:06:90	1	1	Dynamic
2	00:03:6D:F7:80:7F	2	1	Dynamic

There are total 2 Mac Addresses.

Figure 4-6-1: Dynamic MAC Address interface

MAC Table Columns

Object	Description
• NO	The MAC address index entry.
• MAC	The MAC address of the entry.
• PORT	The ports that are members of the entry.
• VID	The VLAN ID of the entry.
• Type	Indicates whether the entry is a static or dynamic entry.

Click "**Clear**" to clear the dynamic MAC addresses information of the current port shown on the screen.

4.6.2 Static MAC Table

You can add a static MAC address that remains in the IP DSLAM's address table regardless of whether the device is physically connected to the IP DSLAM. This saves the IP DSLAM from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / delete a static MAC address.

■ Add the Static MAC Address

You can add static MAC address in the IP DSLAM MAC table here.

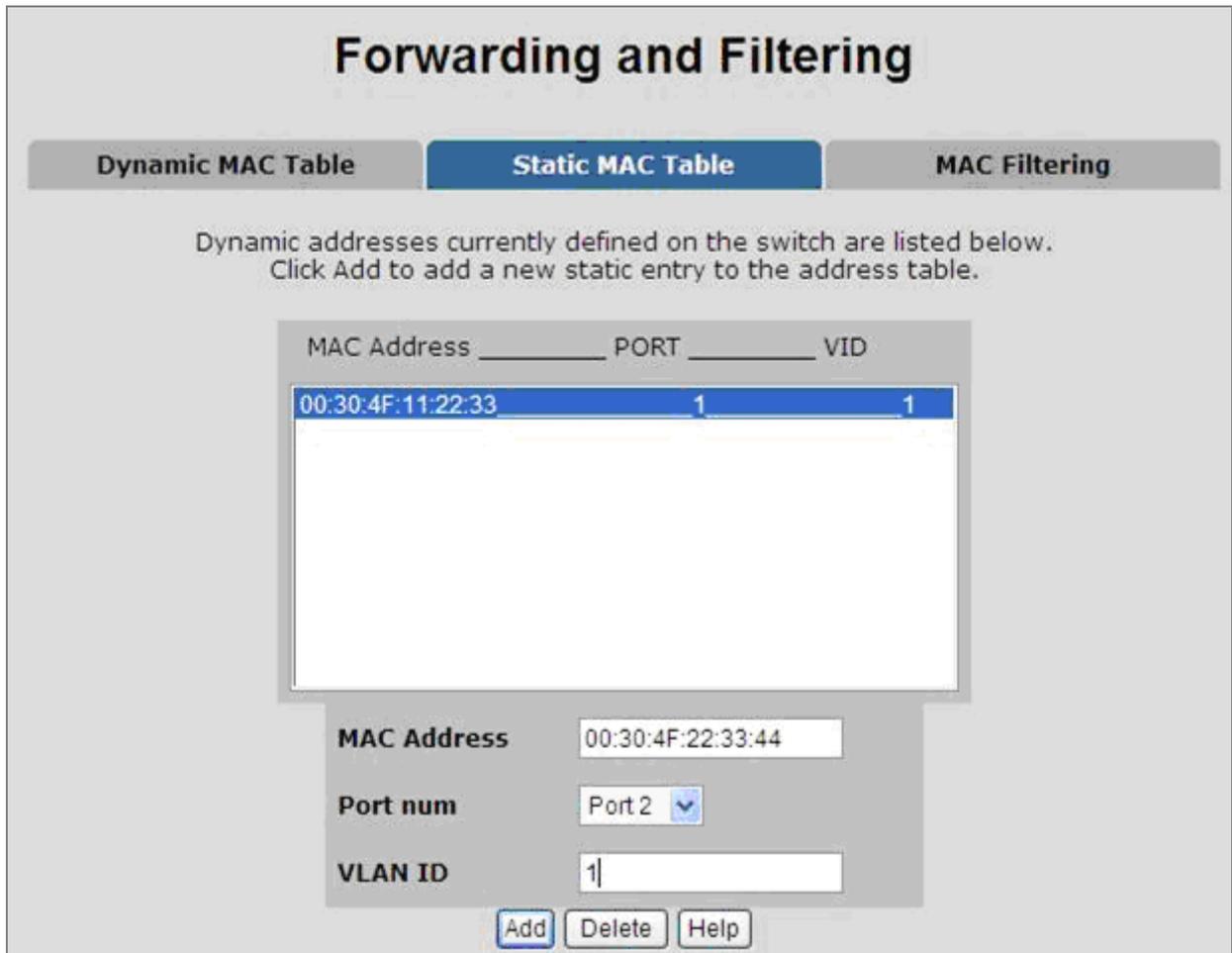


Figure 4-6-2: Static MAC Addresses interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
Port num.:	Pull down the selection menu to select the port number.
VLAN ID:	The VLAN ID for the entry.

4.6.3 MAC Filtering

By filtering MAC address, the IP DSLAM can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

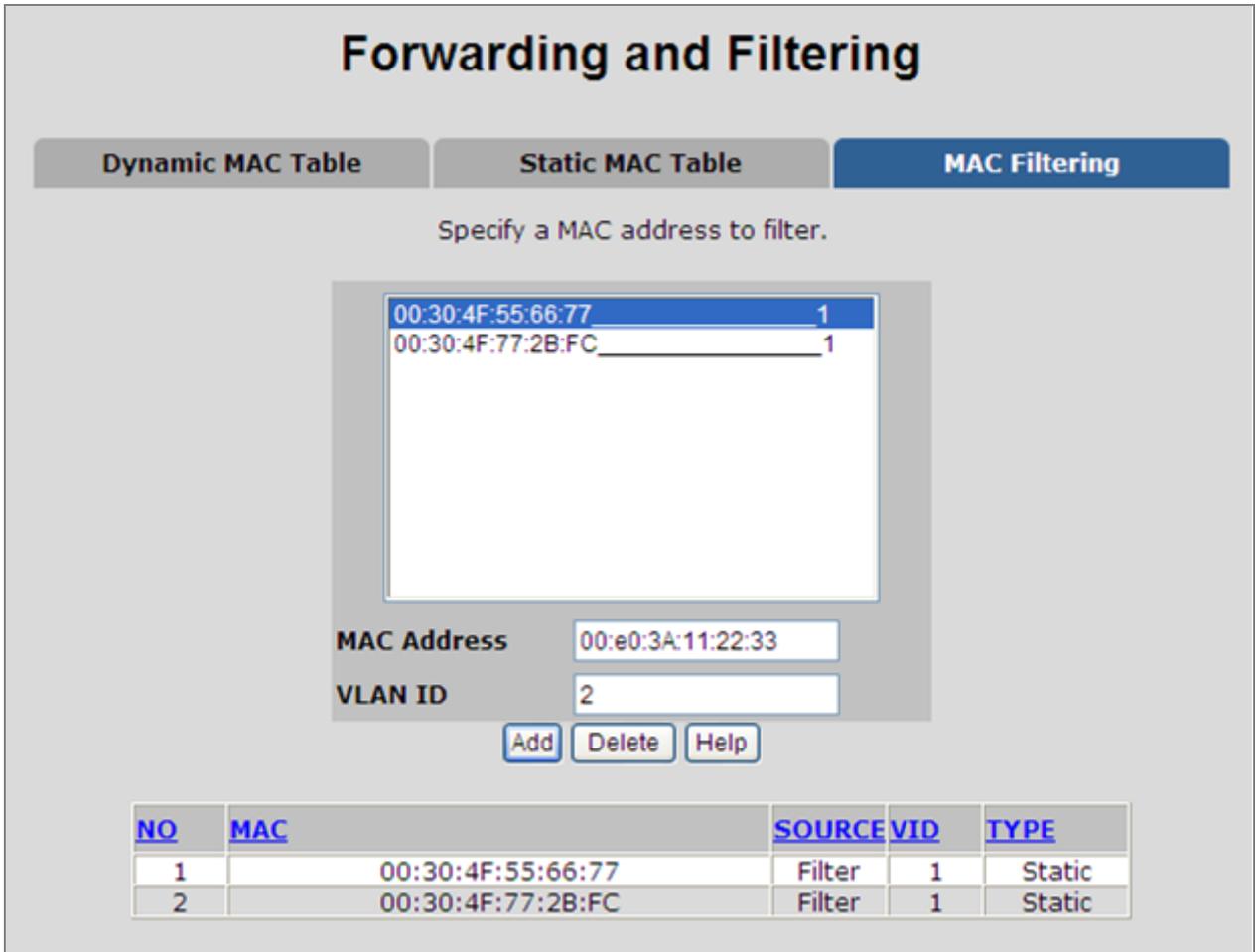


Figure 4-6-3: MAC Filtering interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address that you want to filter.
VLAN ID:	The VLAN ID for the entry.

4.7 IGMP Snooping

4.7.1 Theory

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a DSLAM feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given sub network. If there are no members on a sub network, packets will not be forwarded to that sub network.

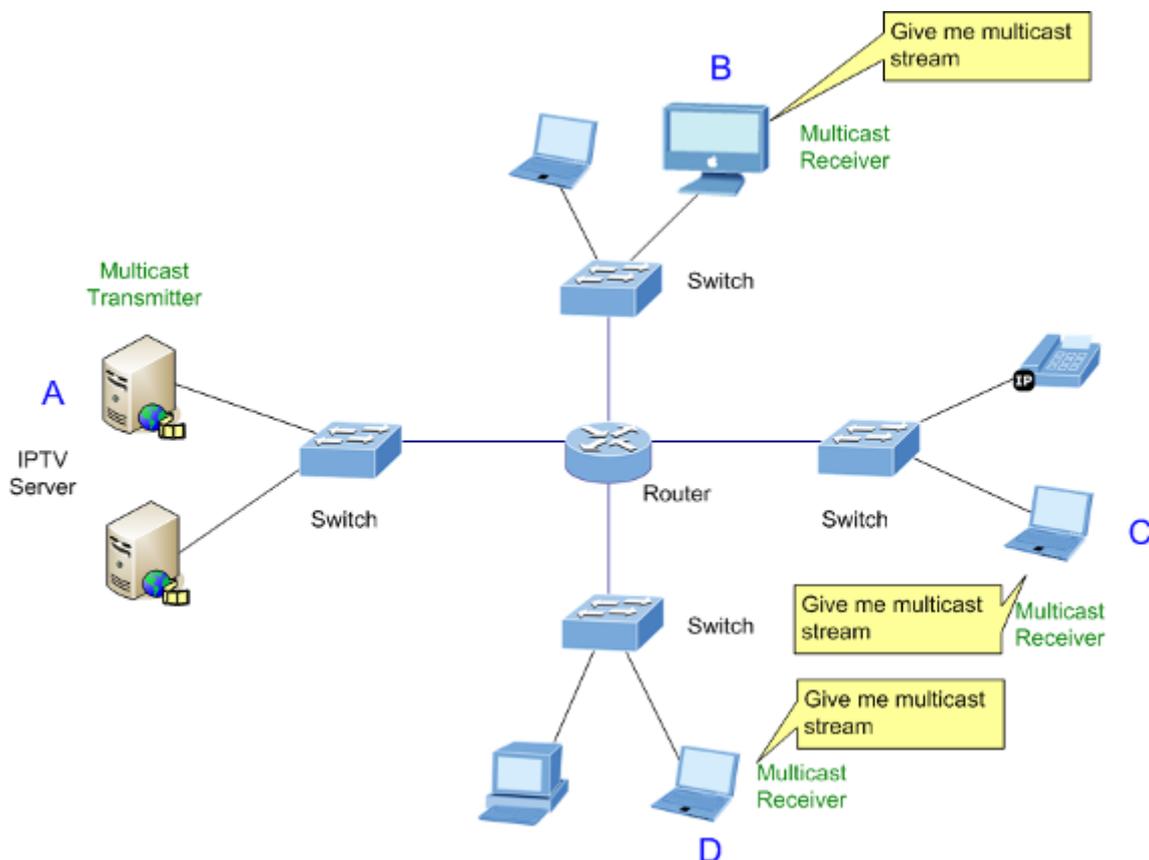


Figure 4-7-1: Multicast Service

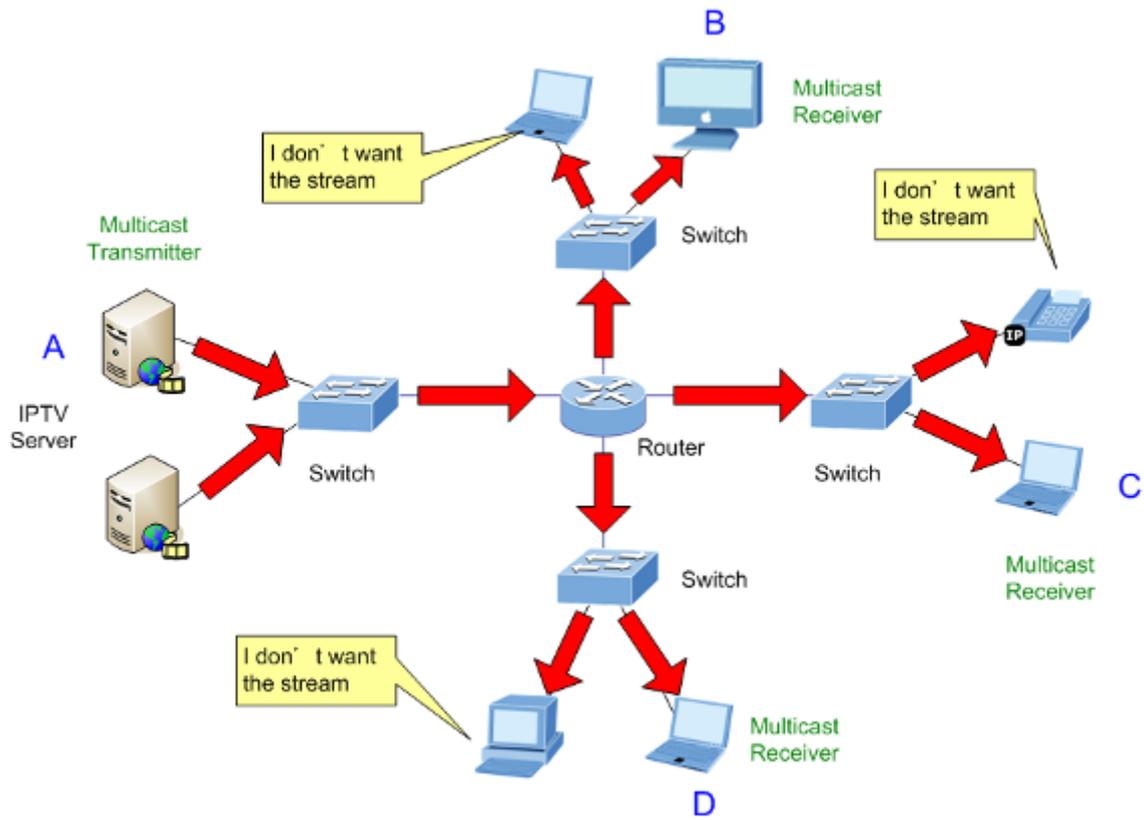


Figure 4-7-2: Multicast flooding

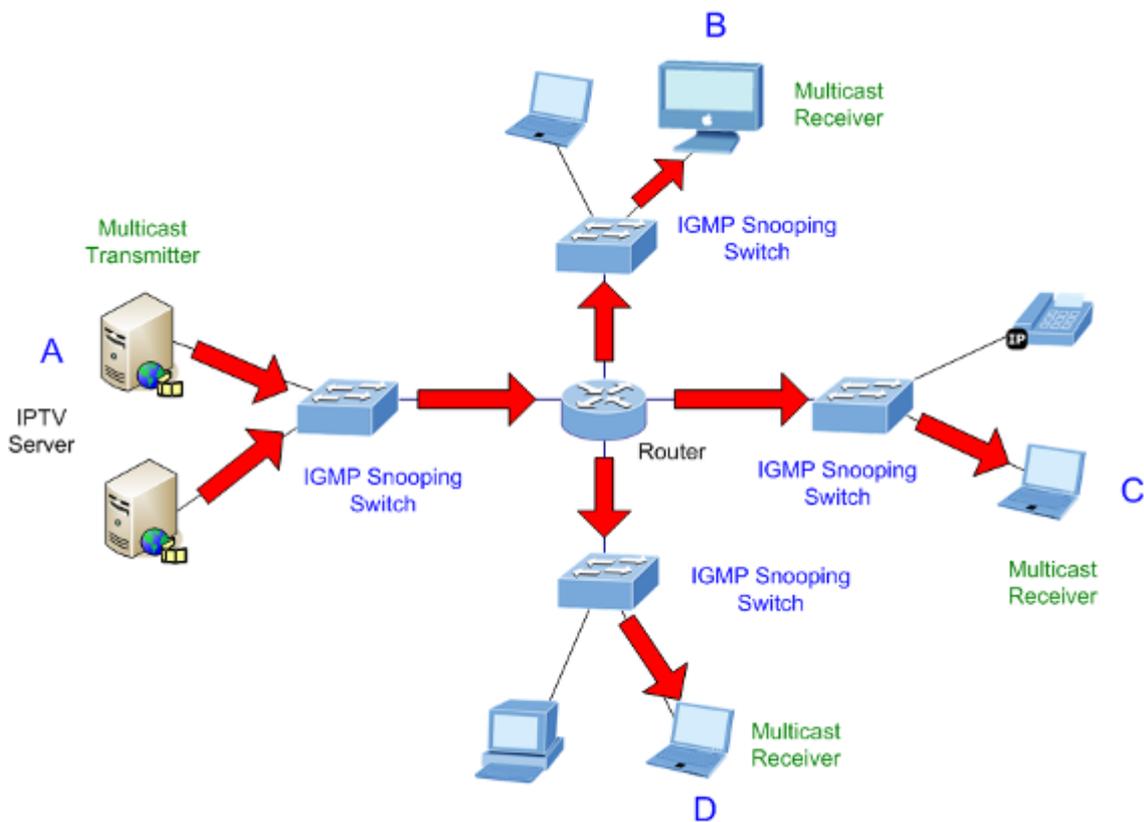


Figure 4-7-3: IGMP Snooping multicast stream control

IGMP Versions 1 and 2

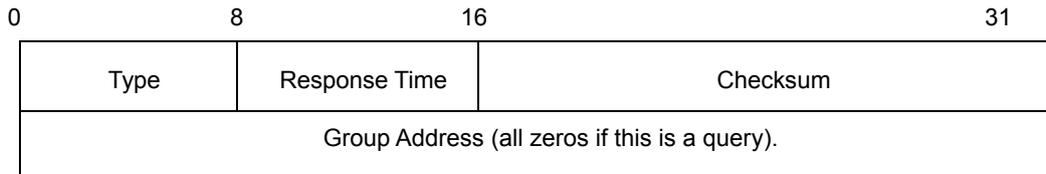
Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets



The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0).
0x11	Specific Group Membership Query (if Group Address is Present).
0x16	Membership Report (version 2).
0x17	Leave a Group (version 2).
0x12	Membership Report (version 1).

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP “**report**” to join a group.

A host will never send a report when it wants to leave a group (for version 1).

A host will send a “**leave**” report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

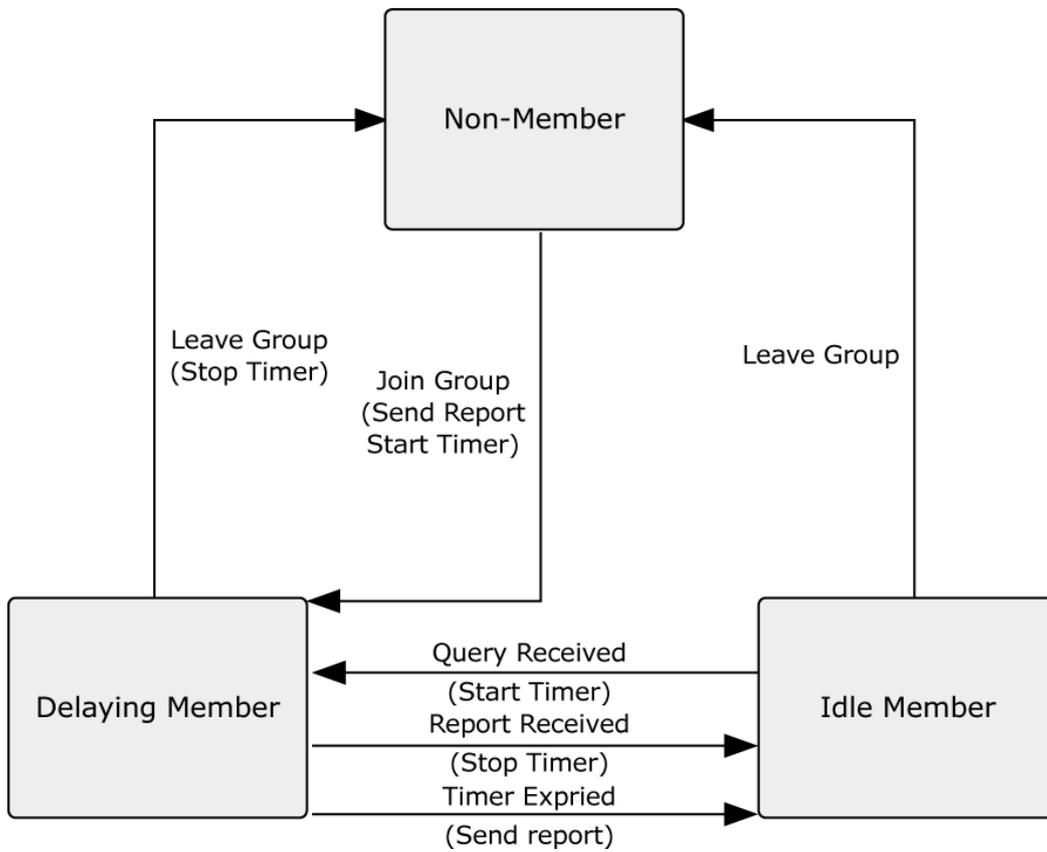


Figure 4-7-4: IGMP State Transitions

■ **IGMP Querier**

A router, or multicast-enabled DSLAM, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router / DSLAM on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast DSLAM/router to ensure that it will continue to receive the multicast service.



Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.7.2 IGMP Configuration

The IP DSLAM support IP multicast, you can enable IGMP protocol on web management's DSLAM setting advanced page, then the IGMP snooping information displays. IP multicast addresses range are from **224.0.0.0** through **239.255.255.255**.

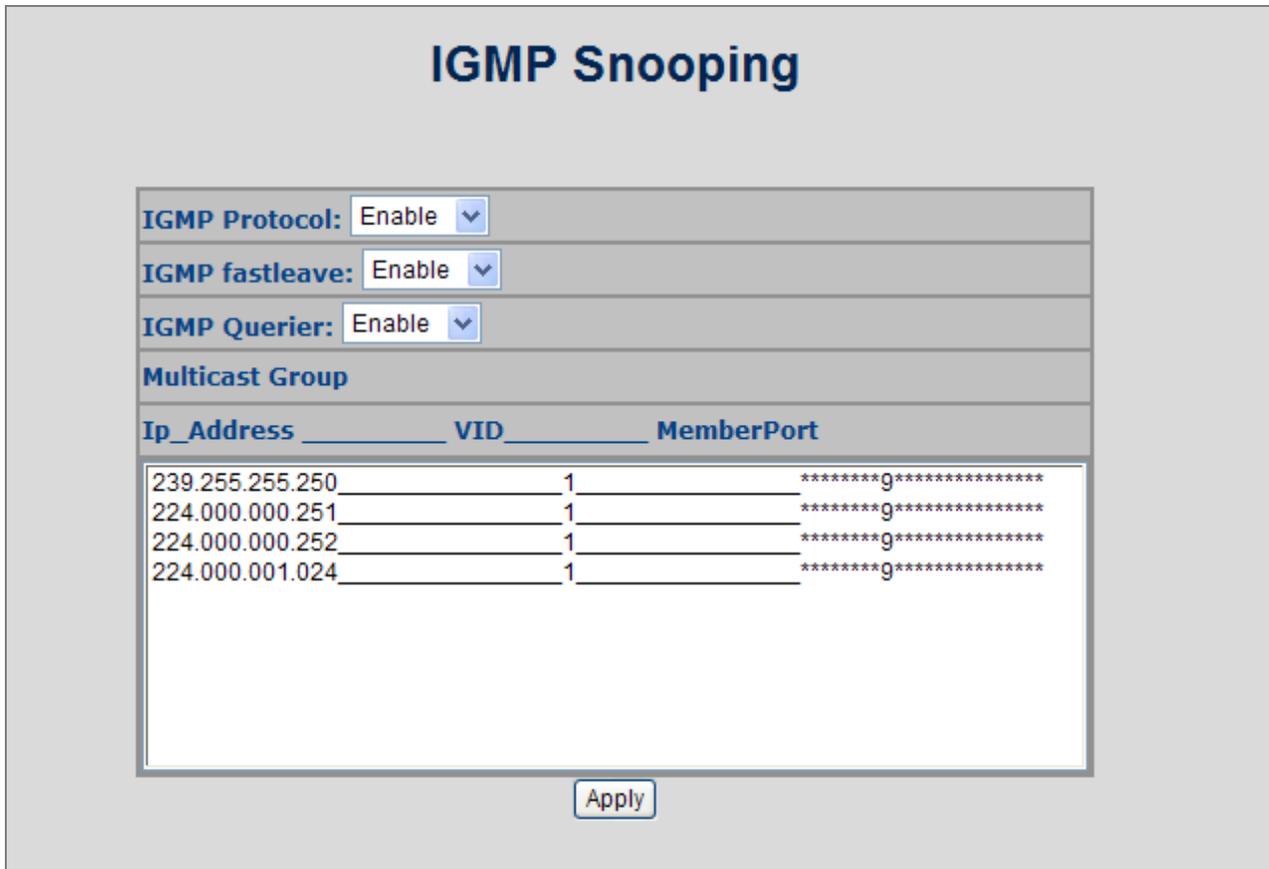
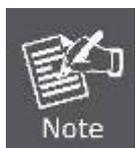


Figure 4-7-5: IGMP Configuration interface

The page includes the following fields:

Object	Description
IGMP Protocol:	Enable or disable the IGMP protocol.
IGMP Fast leave:	Enable or disable Fast Leave on the port.
IGMP Querier:	Enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.

Fast Leave:



The IP DSLAM can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the fast leave function is enabled for the parent VLAN. This allows the Managed witch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

4.8 Spanning Tree Protocol

4.8.1 Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the IP DSLAM to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this The IP DSLAM include these versions:

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

STP - The Spanning Tree Protocol (STP) is a standardized method (**IEEE 802.1D**) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

MSTP - The Multiple Spanning Tree Protocol (MSTP) is a standardized method (**IEEE 802.1S**) for providing simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP , or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent **Multiple Spanning Tree Instance (MSTI)**, within **Multiple Spanning Tree (MST)** Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single **Common Spanning Tree (CST)**.

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1s Multiple Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The IP DSLAM STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single DSLAM, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique DSLAM identifier
- The path cost to the root associated with each DSLAM port
- The port identifier

STP communicates between switches on the network using **Bridge Protocol Data Units (BPDUs)**. Each BPDU contains the following information:

- The unique identifier of the IP DSLAM that the transmitting DSLAM currently believes is the root DSLAM.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The IP DSLAM sends BPDUs to communicate and construct the spanning-tree topology. All DSLAMs connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the IP DSLAM, but the receiving DSLAM uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One DSLAM is elected as the **root DSLAM**.
- The shortest distance to the root DSLAM is calculated for each DSLAM.
- A **designated DSLAM** is selected. This is the IP DSLAM closest to the root DSLAM through which packets will be forwarded to the root.
- A port for each DSLAM is selected. This is the port providing the best path from the IP DSLAM to the root DSLAM.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all DSLAMs have STP enabled with default settings, the IP DSLAM with the lowest MAC address in the network will become the root DSLAM. By increasing the priority (lowering the priority number) of the best DSLAM, STP can be forced to select the best DSLAM as the root DSLAM.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a DSLAM using STP exists in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets.
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding** – the port is forwarding packets.
- **Disabled** – the port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (DSLAM boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.

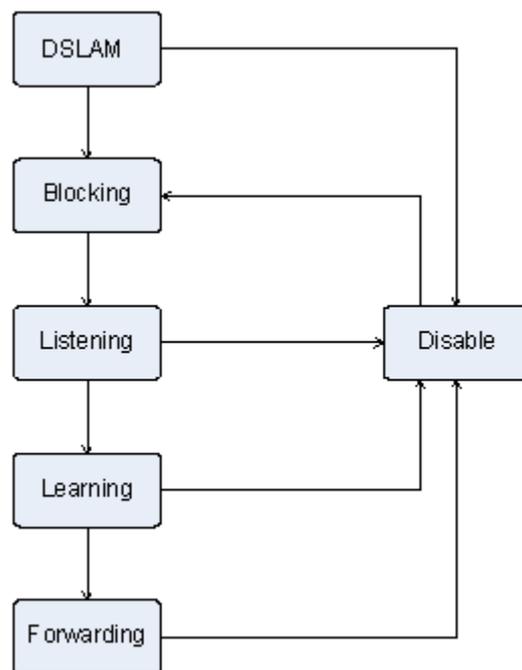


Figure 4-8-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every DSLAM in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

4.8.2 Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

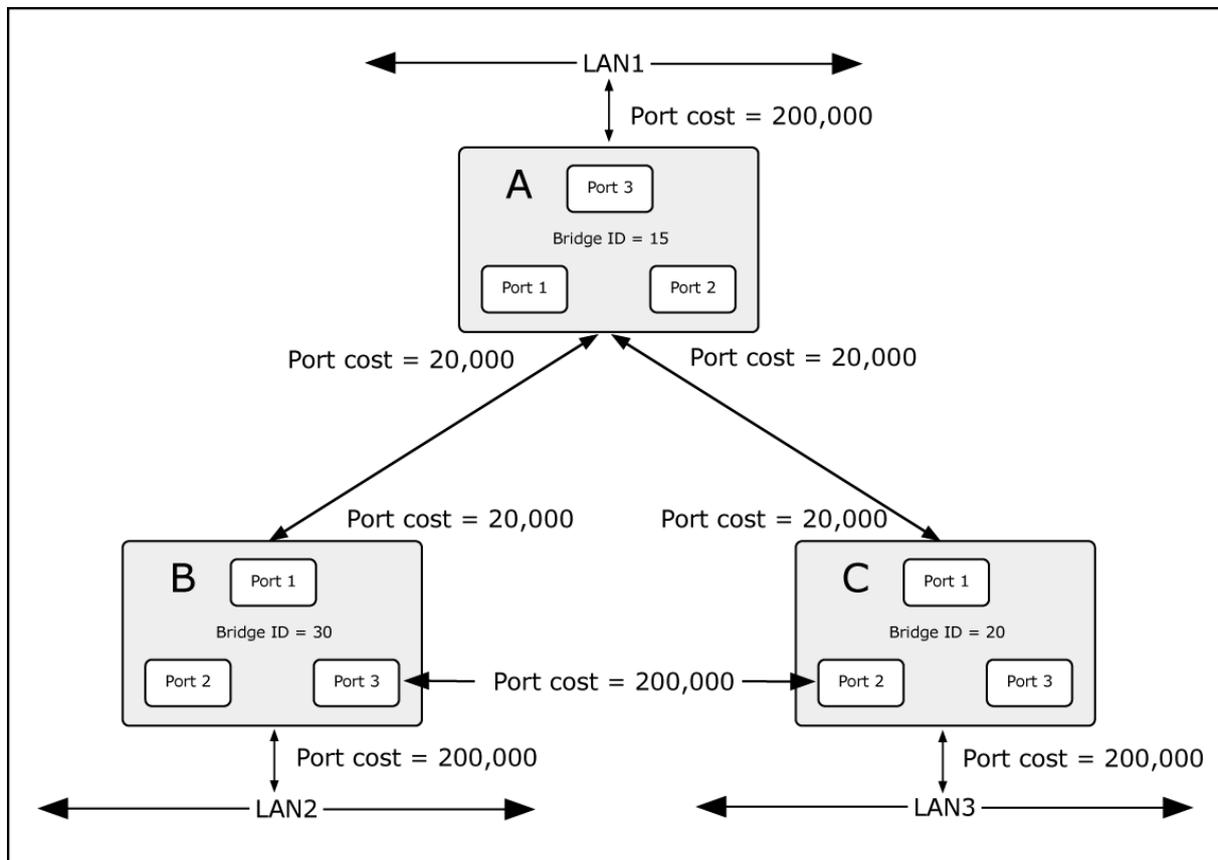


Figure 4-8-2: Before Applying the STA Rules

If DSLAM A broadcasts a packet to DSLAM B, DSLAM B will broadcast it to DSLAM C, and DSLAM C will broadcast it to back to DSLAM A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between DSLAM B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if DSLAM A broadcasts a packet to DSLAM C, then DSLAM C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular DSLAM as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

In this example, only the default STP values are used.

The IP DSLAM with the lowest Bridge ID (DSLAM C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on DSLAM A are connected to one (optional) Gigabit port on both DSLAM B and C. The redundant link between DSLAM B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between DSLAM B and DSLAM C is the blocked link.

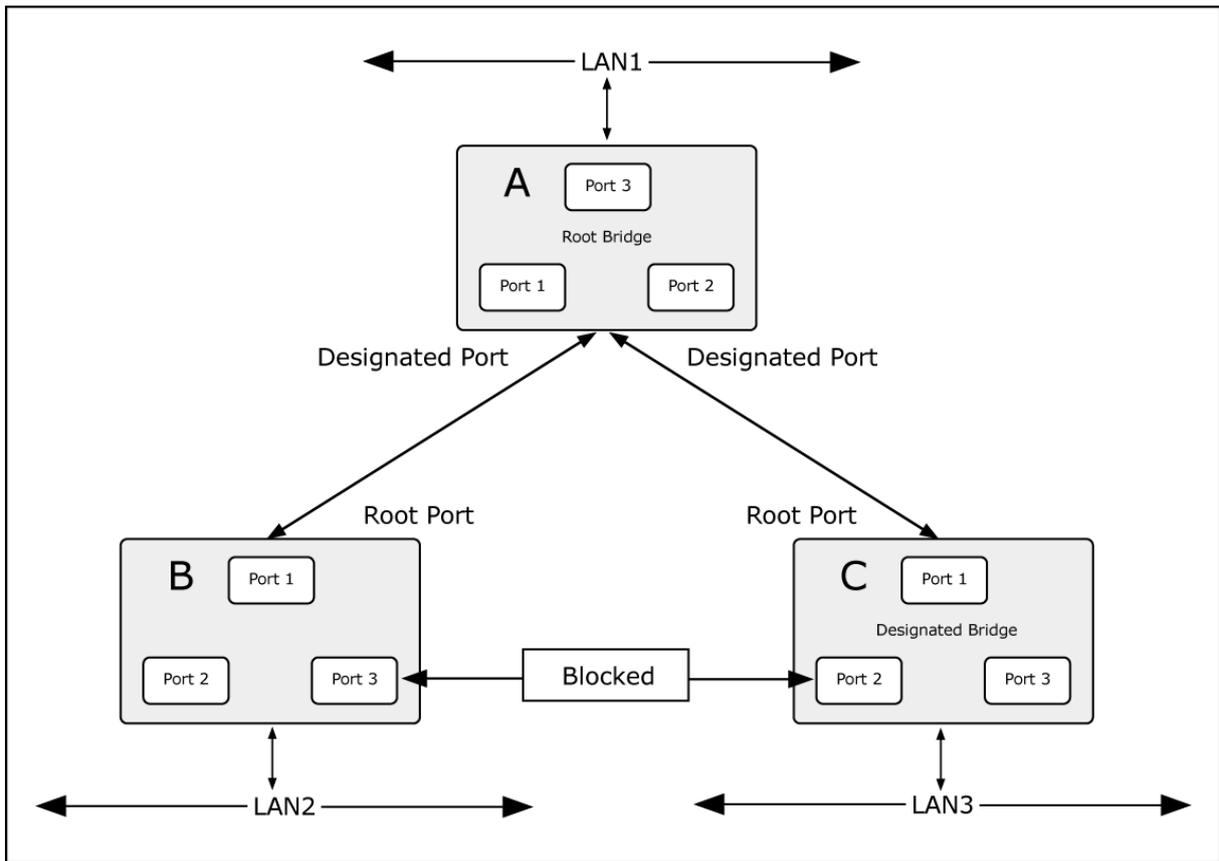


Figure 4-8-3: After Applying the STA Rules

4.8.3 STP Parameters

STP Operation Levels

The IP DSLAM allows for two levels of operation: the IP DSLAM level and the port level. The IP DSLAM level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.



On the IP DSLAM level, STP calculates the Bridge Identifier for each DSLAM and then sets the Root Bridge and the Designated Bridges.
 On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the IP DSLAM level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the IP DSLAM's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC

Priority	A relative priority for each DSLAM – lower numbers give a higher priority and a greater chance of a given DSLAM being elected as the root bridge.	32768
Hello Time	The length of time between broadcasts of the hello message by the IP DSLAM.	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

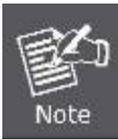
Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port.	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768



The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.



Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

4.8.4 STP System Configuration

This section provides STP-System Configuration from the IP DSLAM, the screen in [Figure 4-8-4](#) appears.

- The user can view spanning tree information of Root Bridge.
- The user can modify STP state. After modification, click **Apply**.

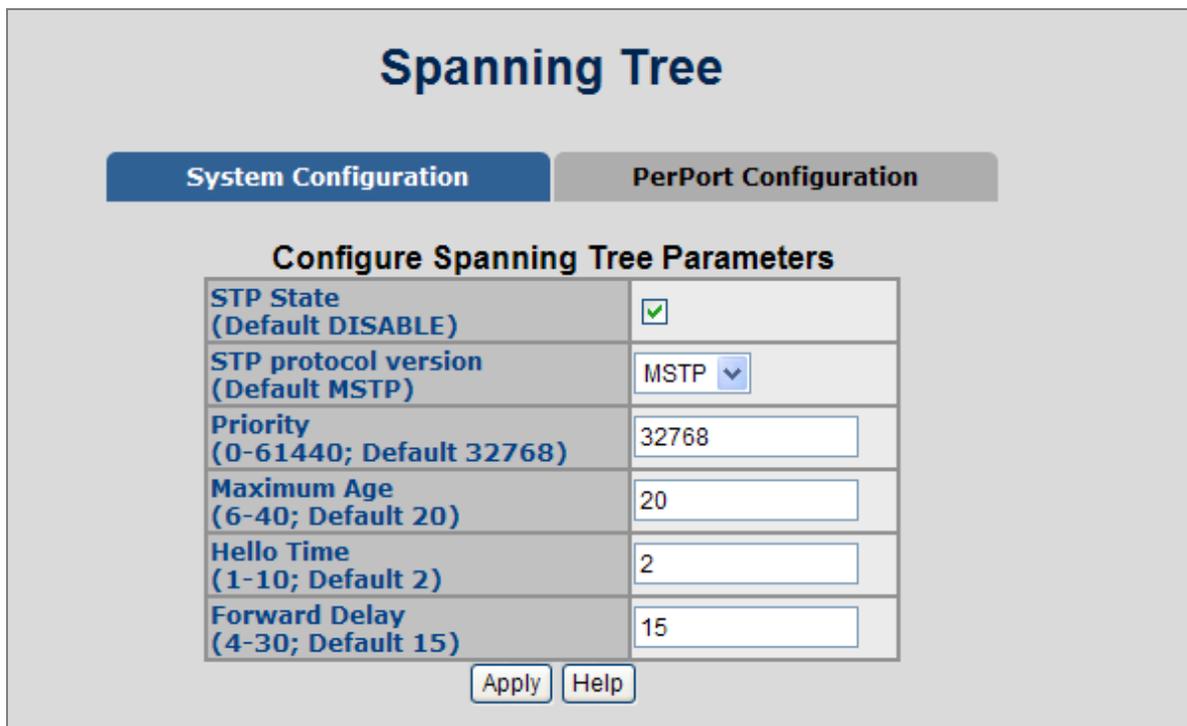


Figure 4-8-4: STP System Configuration interface

The page includes the following fields:

Object	Description
STP State:	The user must enable the STP function first before configuring the related parameters.
Protocol Version	A value used to specify the spanning tree protocol, the original spanning tree protocol (STP, 802.1d) or the multiple spanning tree protocol (MSTP, 802.1s).
Priority (0-61440):	The IP DSLAM with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the IP DSLAM. The value must be a multiple of 4096 according to the protocol standard rule.

Max Age (6-40):	The number of seconds a DSLAM waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10):	The time that controls the IP DSLAM to send out the BPDU packet to check STP current status. Enter a value between 1 through 10.
Forward Delay Time (4-30):	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.



Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time.
 $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$.



Each DSLAM in a spanning-tree adopts the Hello Time, Forward Delay time, and Max Age parameters of the root bridge, regardless of how it is configured.

■ Root Bridge Information

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

The STP Bridge Status screen in [Figure 4-8-5](#) appears.

Priority	32768
MAC Address	00:30:4F:26:20:D1
Root Path Cost	0
Root Port	PORT140
Maximum Age	20
Hello Time	2
Forward Delay	15

Figure 4-8-5: STP Bridge Status page screenshot

The page includes the following fields:

Object	Description
Priority	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
MAC Address	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Root Port	The IP DSLAM port currently assigned the <i>root</i> port role.
Maximum Age	Path Cost to the Designated Root for the Root Bridge.
Hello Time	Minimum time between transmissions of Configuration BPDUs.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.

4.8.5 Port Configuration

This web page provides the port configuration interface for STP. You can assign higher or lower priority to each port. Spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

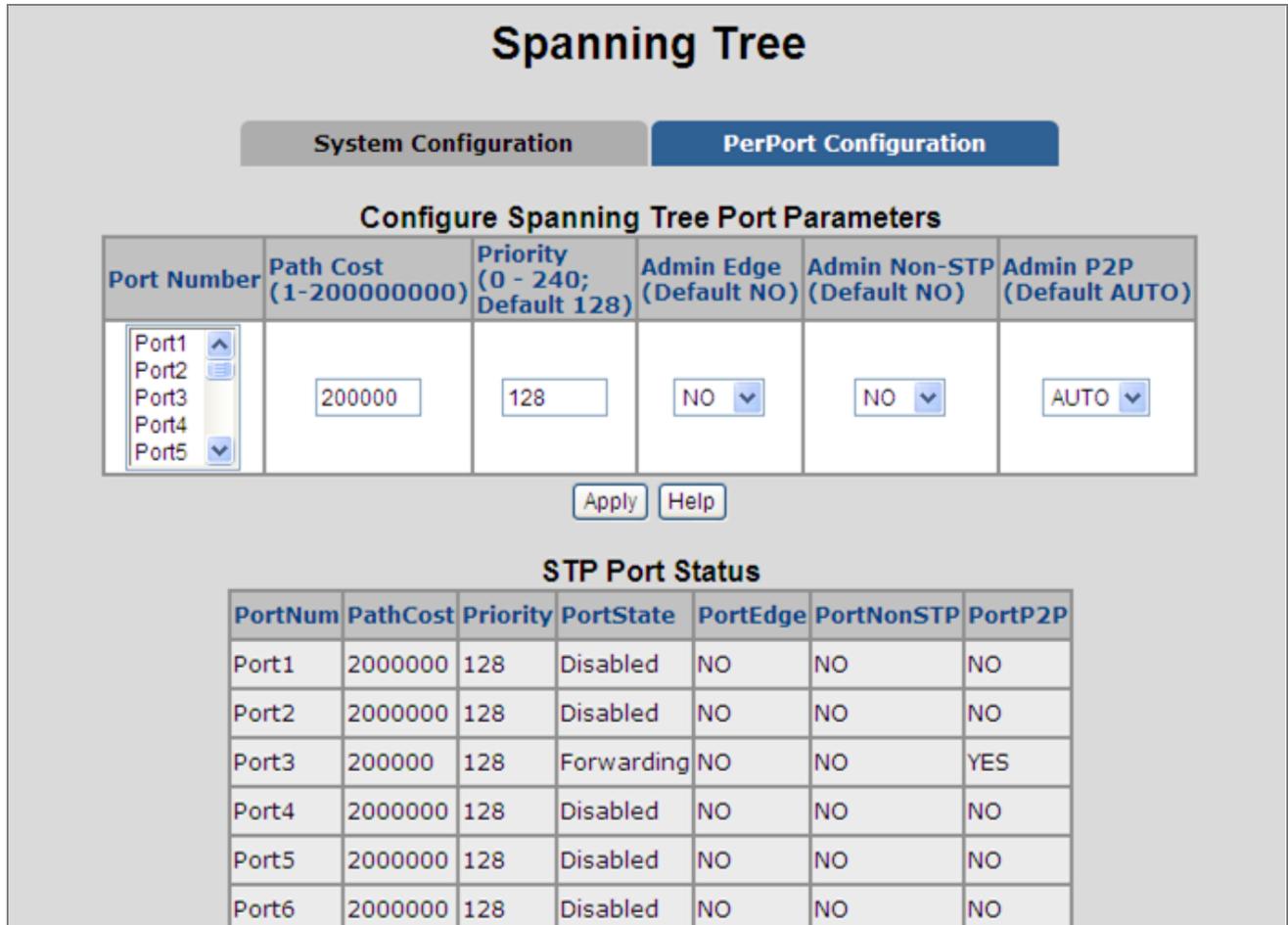


Figure 4-8-6: STP Port Configuration interface

The page includes the following fields:

Object	Description
Path Cost:	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000 .
Priority:	Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240 . The value of priority must be the multiple of 16.

Admin P2P:

The rapid state transitions possible within STP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively.

- **YES** means the port is regarded as a point-to-point link.
- **NO** means the port is regarded as a shared link.
- **AUTO** means the link type is determined by the auto-negotiation between the two peers.

Admin Edge:

The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "YES" status.

Admin Non STP:

The port includes the STP mathematic calculation.

- **YES** is not including STP mathematic calculation.
- **NO** is including the STP mathematic calculation.



Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-8-1: Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 4-8-2: Recommended STP Path Costs

4.9 DHCP Relay & Option 82

The Relay Agent Information option (**Option82**) is inserted by the **DHCP relay** agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies.

The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

Configuring DHCP Relay & Option82

To configure DHCP Option82

1. Enable global option82 function: select DHCP Option82 enable "Enable".
2. Enable port option82 function: select Option82 checkbox for special port.
3. Select DHCP Router Port.
4. Click Apply.

To configure DHCP Relay

5. Enable global Relay function: select DHCP Relay enable "Enable".
6. Enable port Relay function: Type the IP addresses of the DHCP "Relay IP".
7. DHCP Server offers an IP address to client from its list of scopes, which subnet is same as the Relay IP.
8. Select DHCP Router Port.
9. Click Apply.

DHCP Relay & Option 82

DHCP Option 82 Disable ▾		
DHCP Relay Disable ▾		
DHCP Option 82 Router Port None ▾		
DHCP Opt.82 Port	Option	Relay IP
Port1	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port2	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port3	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port4	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port5	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port6	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port7	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port8	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port9	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port10	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port11	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port12	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port13	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port14	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port15	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>

Figure 4-9-1: DHCP Relay & Option 82

The page includes the following fields:

Object	Description
DHCP Option 82	Enable global option82 function
DHCP Relay	Enable global Relay function
DHCP Option 82 Router Port	Select the Router Port that is used to connect to the DHCP server in the domain
DCHP Opt.82 Port	Identify Port-1 to Port-26 to configure DHCP option 82
Option	Enable port option82 function on selected port.
Relay IP	Type the IP addresses of the DHCP "Relay IP".

4.10 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

4.10.1 LLDP Configuration

Use this page to change LLDP parameters.

Figure 4-10-1: LLDP Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP hello time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP hold time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.

4.10.2 PerPort Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in [Figure 4-10-2](#) appears.

LLDP Configuration

LLDP Configuration
PerPort Configuration

Configure Port Status

Port Number	Port Status
<div style="border: 1px solid #ccc; padding: 2px;"> Port1 ▲ Port2 ▢ Port3 ▢ Port4 ▢ Port5 ▼ </div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Tx_only ▼</div>

Port Status

PortNum	Status
Port1	Tx_and_Rx
Port2	Tx_and_Rx
Port3	Tx_and_Rx
Port4	Tx_and_Rx

Figure 4-10-2: LLDP per port Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP hello time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP hold time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.
Port Status	You can change LLDP port status to Tx_only/Rx_only/Tx_and_Rx/Disable. Tx_only: LLDP transmit the packet of the port only. Rx_only: LLDP receive the packet of the port only. Tx_and_Rx: LLDP transmit and receive the packets of the port. Disable: LLDP do not transmit and receive the packets of the port.

4.11 Access Control List

The **Access Control List (ACL)** is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identifier. **Access Control List (ACL)** is a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted or denied to access the resource. The screen in following screen appears.

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The IP DSLAM can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

※Packet Type / Binding§ can be selected to ACL for IPv4 or Non-IPv4.

Access Control List

Group Id	<input type="text" value=""/> (1~200)		
Action	Permit <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)		
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094;Any means Vid=0 if uses binding)		
Packet Type / Binding	<input checked="" type="radio"/> IPv4 <input type="radio"/> Non-IPv4 <input type="radio"/> Binding		
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/>	Ether Type	Any <input type="text" value=""/> Type# <input type="text" value=""/>
	Mask <input type="text" value="255.255.255.255"/>		MAC Address <input type="text" value="00:11:22:33:44:55"/>
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/>	IP Address	<input type="text" value="0.0.0.0"/>
	Mask <input type="text" value="255.255.255.255"/>		Port Id <input type="text" value="1"/> (1~26)
IP Fragment	<input type="checkbox"/> Uncheck <input type="checkbox"/>		
L4 Protocol	<input checked="" type="radio"/> Any <input type="radio"/> TCP <input type="text" value="Any"/>	QOS VoIP	Priority# <input type="text" value="7"/>
	Protocol#: <input type="text" value=""/>		PortID# <input type="text" value="0"/> Value (Hex,0~1F) <input type="text" value=""/> Mask (Hex,0~1F) <input type="text" value="0"/>
	<input type="radio"/> UDP <input type="text" value="Any"/>		Protocol# <input type="text" value="0"/> Value (Hex,0~FF) <input type="text" value=""/> Mask (Hex,0~FF) <input type="text" value="0"/>
	Port#: <input type="text" value=""/>		Source Port# <input type="text" value="0"/> Value (Hex,0~FFFF) <input type="text" value=""/> Mask (Hex,0~FFFF) <input type="text" value="0"/>
	Port#: <input type="text" value=""/>		Destination Port# <input type="text" value="0"/> Value (Hex,0~FFFF) <input type="text" value=""/> Mask (Hex,0~FFFF) <input type="text" value="0"/>
Port Id	<input type="text" value="0"/> (1~26,0: don't care)		
Current List	<div style="border: 1px solid gray; height: 40px;"></div>		

Figure 4-11-1: Access Control List (ACL) Web Page screen

The page includes the following fields:

■ IPv4 ACL

Object	Description	Default Value
Group ID	1 ~ 200 (max. 200 ACL group).	
Action	Permit / Deny. <ul style="list-style-type: none"> ■ Permit: Permit packet cross DSLAM. ■ Deny: Drop packet. 	Permit
VLAN	Any / VID. <ul style="list-style-type: none"> ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID. 	Any
Packet Type	IPv4 / Non-IPv4 / Binding <ul style="list-style-type: none"> ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry. 	IPv4
Src IP Address	Set this field if Packet Type is IPv4, else ignore. Any / IP and Mask <ul style="list-style-type: none"> ■ Any: Any IP address. ■ IP: A certain IP address. Mask: *.*.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255 Notice: This is not subnet mask.	Any
Dst IP Address	Set this field if Packet Type is IPv4, else ignore. Any / IP and Mask <ul style="list-style-type: none"> ■ Any: Any IP address. ■ IP: A certain IP address. Mask: *.*.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255	Any
IP Fragment	Set this field if Packet Type is IPv4, else ignore. Uncheck / Check <ul style="list-style-type: none"> ■ Uncheck: Not check IP fragment field. ■ Check: Check IP fragment field. 	Uncheck
L4 Protocol	Set this field if Packet Type is IPv4, else ignore. Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)	Any
Protocol	Set this field if Packet Type is IPv4, else ignore. 0~255. If protocol not find in L4 Protocol field, you can direct assign number.	

TCP	Set this field if Packet Type is IPv4, else ignore. Any / FTP(21) / HTTP(80)	Any
Port	Set this field if Packet Type is IPv4, else ignore. 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	Set this field if Packet Type is IPv4, else ignore. Any / DHCP(67) / TFTP(69) / NetBios(137)	Any
Port	Set this field if Packet Type is IPv4, else ignore. 0~65535 If UDP port not find in UDP field, you can direct assign number.	
Port ID	Source port ID, from 1~26, 0 means don't care.	0
Current List	You create ACL and Binding groups.	

■ Non-IPv4 ACL

In ※Packet Type / Binding box should select ※Non-IPv4

Object	Description	Default Vaule
Group ID	1 ~ 200 (max. 200ACL group)	
Action	Permit / Deny. <ul style="list-style-type: none"> ■ Permit: Permit packet cross DSLAM. ■ Deny: Drop packet. 	Permit
VLAN	Any / VID. <ul style="list-style-type: none"> ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID. 	Any
Packet Type	IPv4 / Non-IPv4 / Binding <ul style="list-style-type: none"> ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry. 	IPv4
Ether Type	Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	Any
Type	Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

■ Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross DSLAM if all conditions match.

Use binding function; we should enable it first in following page.

In ※Packet Type / Binding box should select ※Binding.

Object	Description	Default Vaule
Group ID	1 ~ 200 (max. 200 ACL group)	
Action	Permit / Deny. <ul style="list-style-type: none"> ■ Permit: Permit packet cross DSLAM. ■ Deny: Drop packet. 	Permit
VLAN	Any / VID. <ul style="list-style-type: none"> ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID. 	Any
Packet Type	IPv4 / Non-IPv4 / Binding <ul style="list-style-type: none"> ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry. 	IPv4
MAC Address	**.*.*.*.*.*.*.* * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	00:11:22:33:44:55
IP Address	***.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255.	0.0.0.0
Port ID	Source port ID, from 1~26.	1
Current List	You create ACL and Binding groups.	

4.12 Security Manager

This section provides the User Name and the Password assign or the Password Change of the IP DSLAM, the screen in [Figure 4-12-1](#) appears the User Name and the Password Setting object of VDSL IP DSLAM.

Figure 4-12-1: Security Manager Web Page screen

4.13 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an “opening” is available, the IP DSLAM stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

4.13.1 MAC Limit Configuration

The Layer 2 MAC Limit function can be per-port configured for security management purposes. When the port is in MAC Limit mode, the port will be "locked" without permission of address learning. Only the incoming packets with Source MAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses.

Figure 4-13-1: MAC Limit - Configure MAC Limit

The page includes the following fields:

Object	Description
MAC Limit	Enable or disable MAC limit function for the IP DSLAM.
Port Number	Indicate port 1 to port 24.
Limit	The maximum number of per-port MAC addresses to be learned (1-64, 0 to disable this port's MAC limit function).



MAC Limit is only functioned on VDSL port.

4.13.2 MAC Limit Port Status

This table displays current MAC Limit status of each port.

MAC Limit Port Status	
Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off
Port9	off
Port10	off
Port11	off
Port12	off
Port13	off
Port14	off
Port15	off
Port16	off
Port17	off
Port18	off
Port19	off
Port20	off
Port21	off
Port22	off
Port23	off
Port24	off

Figure 4-13-2: MAC Limit – MAC Limit Port Status

The page includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 24.
Limit	Display the current MAC Limit configuration and status of each port.

4.14 802.1x Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired DSLAM until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

4.14.1 Understanding IEEE 802.1x Port-Based Authentication

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a DSLAM port before making available any services offered by the DSLAM or the LAN.

Until the client is authenticated, 802.1x access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown below.

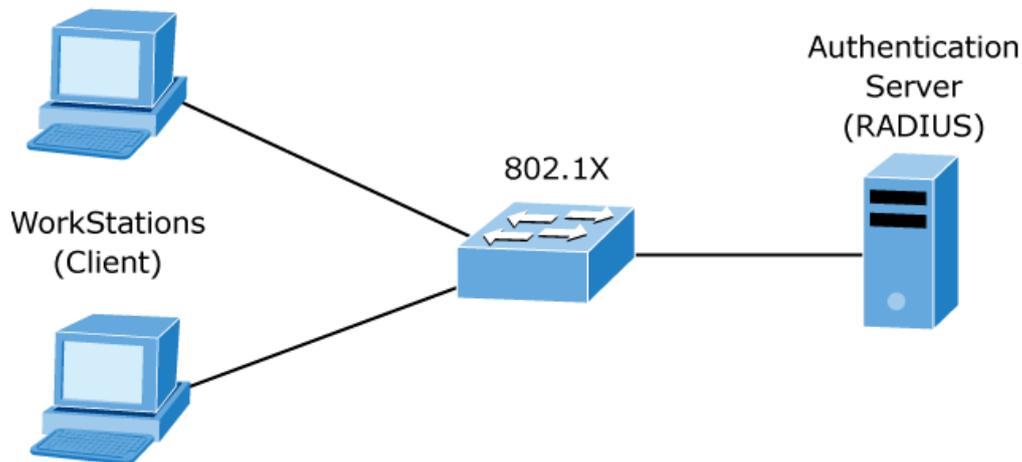


Figure 4-14-1: 802.1x device role

Client—the device (workstation) that requests access to the LAN and DSLAM services and responds to requests from the IP DSLAM. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1x specification.)

- **Authentication server**—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the IP DSLAM whether or not the client is authorized to access the LAN and DSLAM services. Because the IP DSLAM acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible**

Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- **DSLAM (802.1x device)**—controls the physical access to the network based on the authentication status of the client. The IP DSLAM acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The IP DSLAM includes the RADIUS client, which is responsible for encapsulating and encapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the IP DSLAM receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the IP DSLAM receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ Authentication Initiation and Message Exchange

The IP DSLAM or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the IP DSLAM must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the IP DSLAM sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during boot up, the client does not receive an EAP-request/identity frame from the IP DSLAM, the client can initiate authentication by sending an EAPOL-start frame, which prompts the IP DSLAM to request the client's identity.



If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the IP DSLAM begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the IP DSLAM port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. “[Figure 4-14-2](#)” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

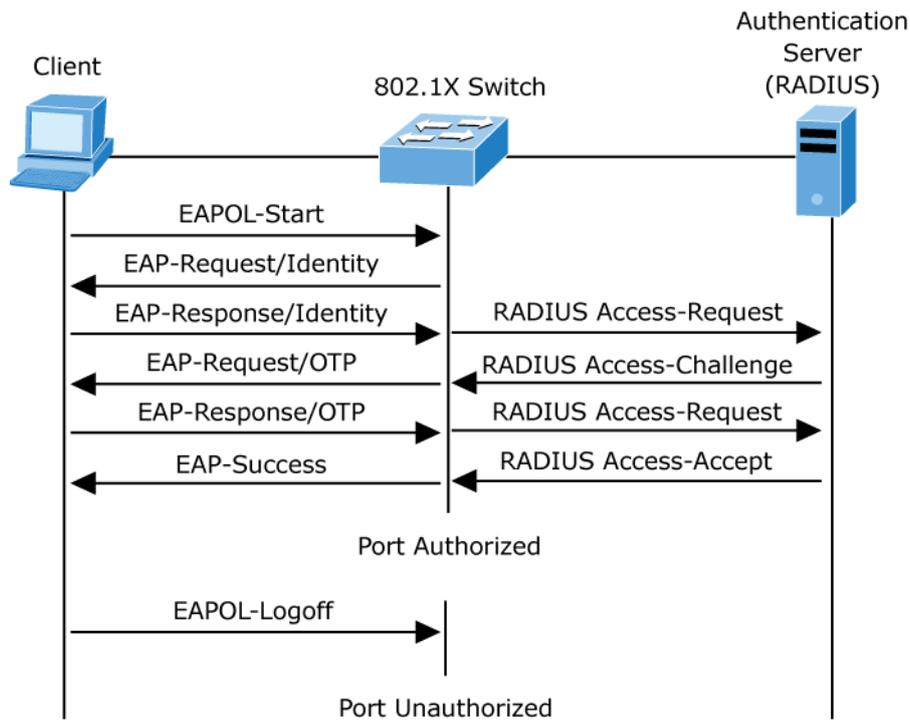


Figure 4-14-2: EAP message exchange

■ Ports in Authorized and Unauthorized States

The IP DSLAM port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the IP DSLAM requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the IP DSLAM can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the IP DSLAM port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.14.2 System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

To enable 802.1x, from **System \ System Information \ Misc Config** then you still to fill in the authentication server information :

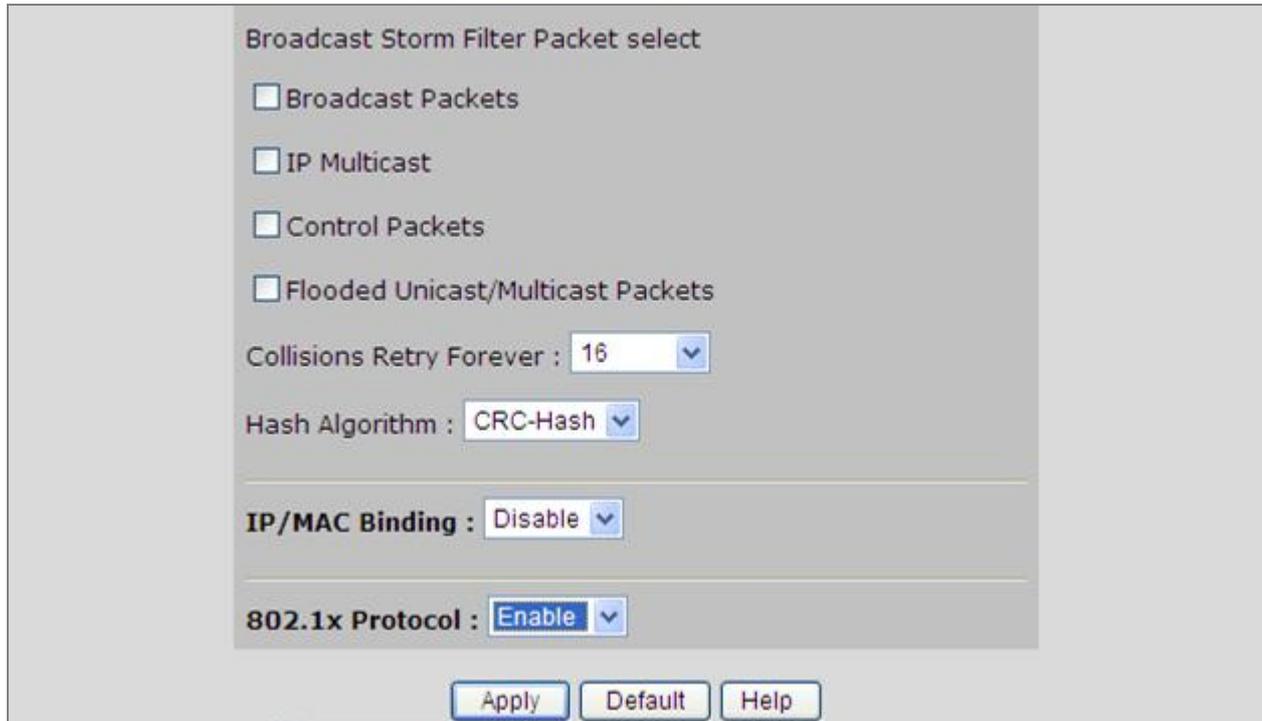


Figure 4-14-3: System information \ Misc Configuration\ 802.1x Protocol

After enabling the IEEE 802.1x function, you can configure the parameters of this function.

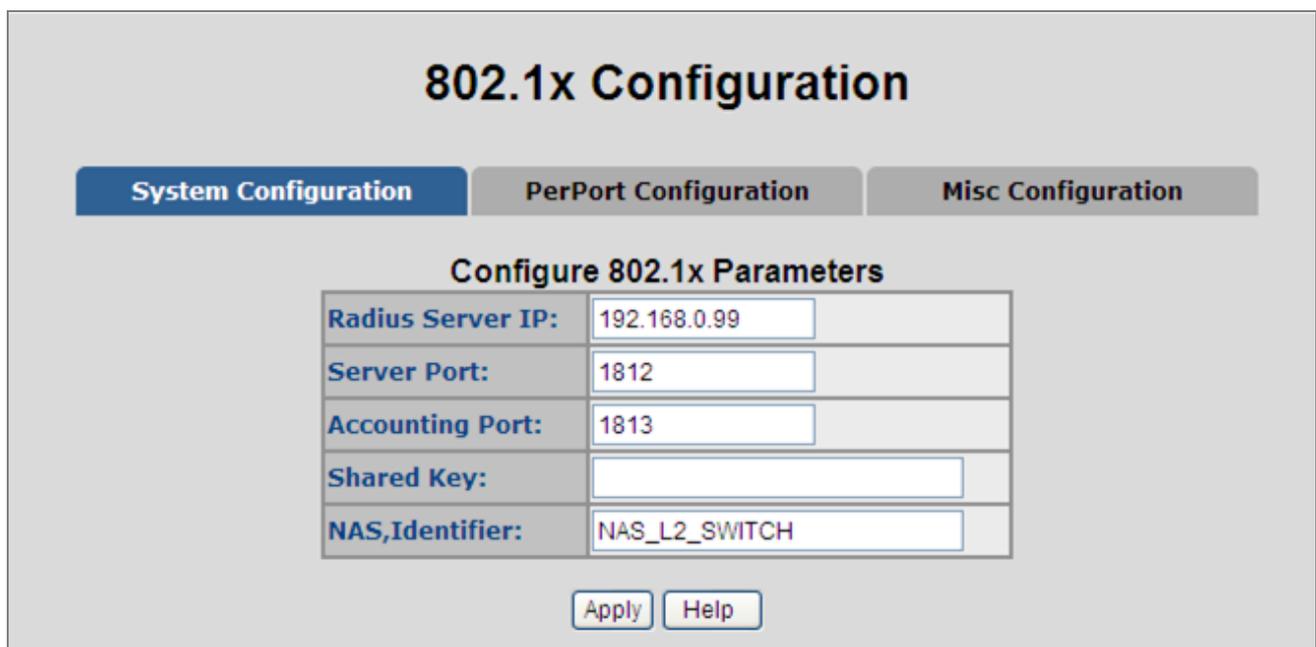


Figure 4-14-4: 802.1x System Configuration interface

The page includes the following fields:

Object	Description
IEEE 802.1x Protocol:	Enable or disable 802.1x protocol.
Radius Server IP:	Assign the RADIUS Server IP address.
Server Port:	Set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port:	Set the UDP destination port for accounting requests to the specified RADIUS Server.
Shared Key:	Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier:	Set the identifier for the RADIUS client.

4.14.3 802.1x Port Configuration

In this page, you can select the specific port and configure the authorization state. The state provides **No Authorization**, **Force Authorized**, **Force unauthorized**, and **Authorize**.

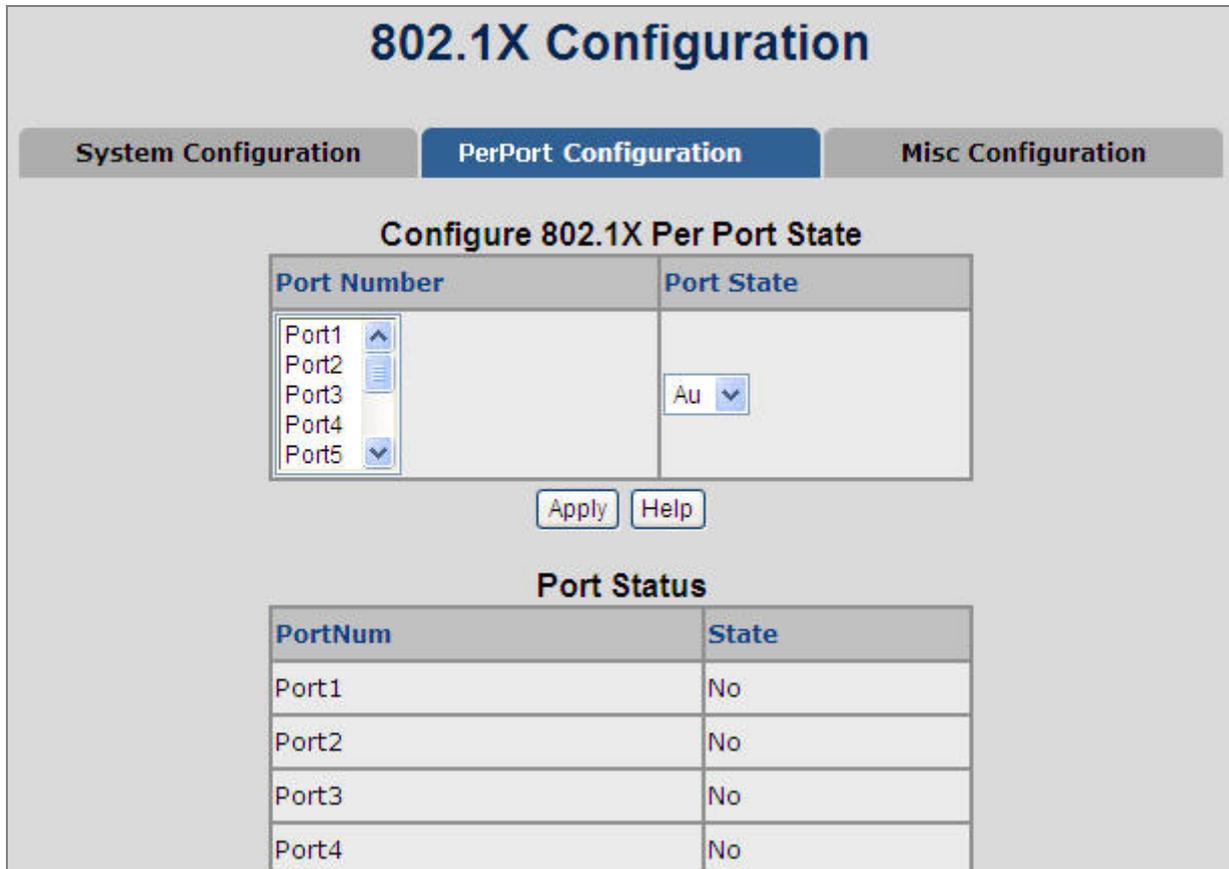


Figure 4-14-5: 802.1x Per Port Setting interface

The page includes the following fields:

Object	Description
Fu (Force Unauthorized)	The specified port is required to be held in the unauthorized state.
Fa (Force Authorized)	The specified port is required to be held in the authorized state.
Au (Authorize)	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
No	The specified port works without complying with 802.1x protocol.

4.14.4 Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:

802.1x Configuration

System Configuration
PerPort Configuration
Misc Configuration

Configure 802.1x misc configuration

Quiet period:	<input type="text" value="60"/>
Tx period:	<input type="text" value="15"/>
Supplicant timeout:	<input type="text" value="30"/>
Server timeout:	<input type="text" value="30"/>
Max requests:	<input type="text" value="2"/>
Reauth period:	<input type="text" value="3600"/>

Figure 4-14-6: 802.1x Misc Configuration interface

The page includes the following fields:

Object	Description
Quiet Period:	Used to define periods of time during which it will not attempt to acquire a supplicant. Default time is 60 seconds.
TX Period:	Set the period the port waits for retransmit next EAPOL PDU during an authentication session. Default value is 30 seconds.
Supplicant Timeout:	Set the period of time the IP DSLAM waits for a supplicant response to an EAP request. Default value is 30 seconds.
Server Timeout:	Set the period of time the IP DSLAM waits for a server response to an authentication request. Default value is 30 seconds.
Max Requests:	Set the number of authentication that must time-out before authentication fails and the authentication session ends. Default value is 2 times.
Reauth period:	Set the period of time which clients connected must be re-authenticated. Default value is 3600 seconds.

4.15 QoS Configuration

4.15.1 Understand QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the IP DSLAM to treat selected applications and types of traffic.

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

The **QoS** page of the IP DSLAM contains three types of QoS mode - the **CoS** mode, **TOS** mode or **Port-based** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **CoS / 802.1p Tag Priority Mode** –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **TOS / DSCP Mode** - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Based Priority Mode** – Any packet received from the specify high priority port will treated as a high priority packet.

4.15.2 QoS Configuration

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When CoS / 802.1p Tag Priority is applied, the IP DSLAM recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

802.1Q Tag and 802.1p priority

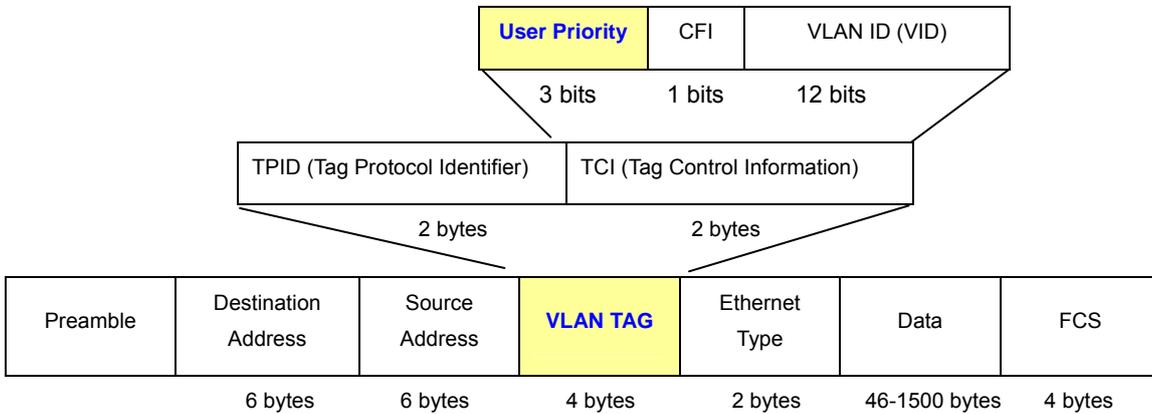


Figure 4-15-1: 802.1p Tag Priority

Set up the COS priority level. With the drop-down selection item of Priority Type above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

4.15.2.1 Priority Queue Service settings

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The IP DSLAM supports Static Port Ingress priority and four queues. The screen in Figure 4-15-2 appears.



Figure 4-15-2: QoS Configuration – 802.1Priority

The table includes the following fields:

Object	Description
First Come First Service	The sequence of packets sent is depending on arrival order.
All High before Low	The high priority packets sent before low priority packets.
Weighted Round Robin	<p>Select the preference given to packets in the DSLAM's higher-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent.</p> <p>For example, 8 Highest : 4 SecHigh : 2 SecLow : 1 Lowest means that the IP DSLAM sends 8 highest priority packets before sending 4 second high priority packet, before sending 2 second low priority packet, before sending 1 lowest priority packet.</p>
802.1p priority [0-7]	Set up the COS priority level 0~7— High, Middle, Low, Lowest .



802.1p Priority: Priority classifiers of the DSLAM forward packet. COS range is from 0 to 7. Seven is the high class. Zero is the less class. The user may configure the mapping between COS and Traffic classifiers.

4.15.2.2 QoS PerPort Configuration

Configure the priority level for each port. With the drop-down selection item of Priority Type above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

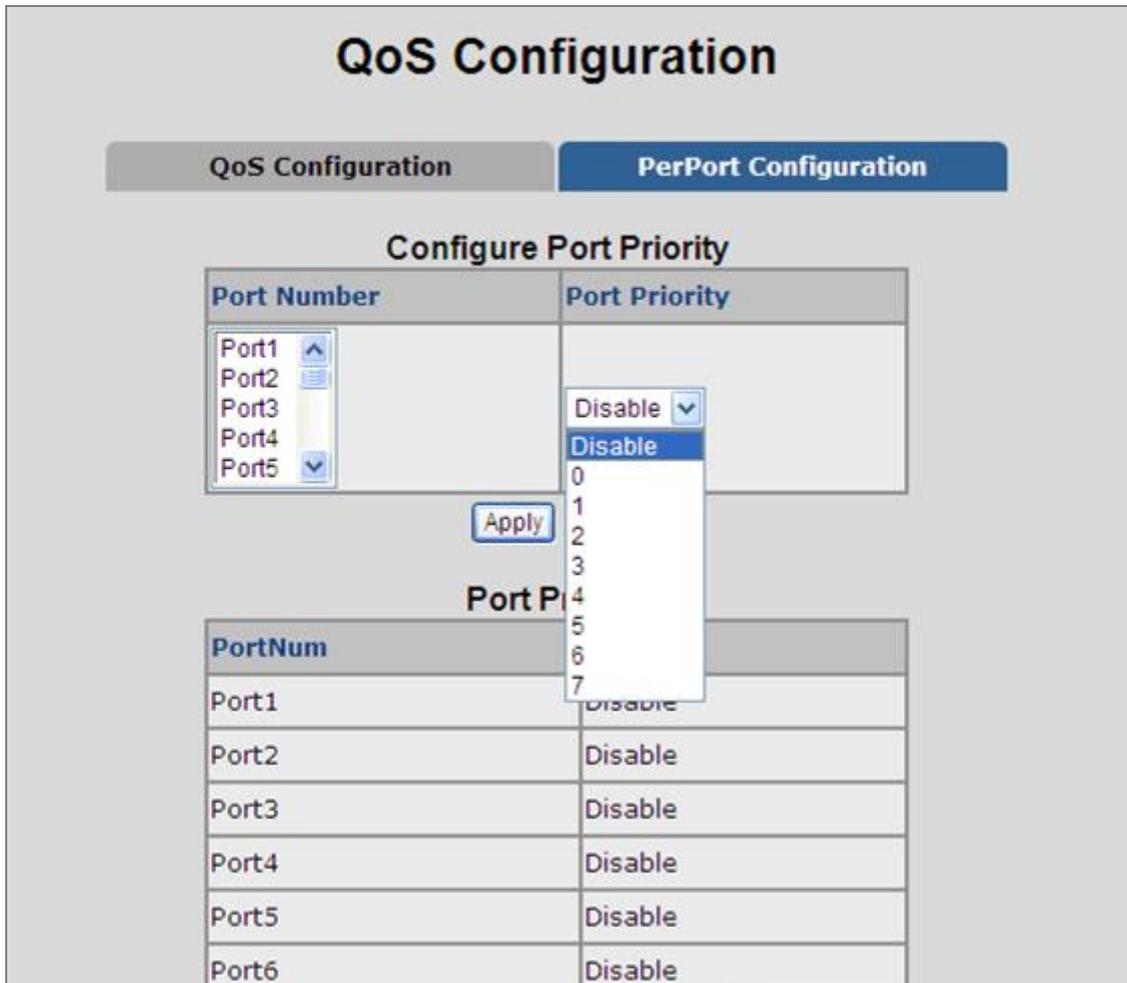


Figure 4-15-3: QoS Configuration – Port-Based Priority

The table includes the following fields:

Object	Description
Port Number:	Indicate port 1 to port 10.
Port Priority:	Each port has 8 priority levels—0~7 or Disable to be chosen. 7 is the highest priority.

4.15.3 TOS/DSCP

TOS/DSCP priority is obtained through a 6-bit **Type-of-Service (TOS)** or **Differentiated Service Code Point (DSCP)** to 3-bit priority mapping.

The **Type of Service (TOS)** octet in the IPv4 header is divided into three parts; Precedence (3 bits), TOS (4 bits), and MBZ (1 bit). The Precedence bits indicate the importance of a packet, whereas the TOS bits indicate how the network should make tradeoffs between throughput, delay, reliability, and cost (as defined in RFC 1394). The MBZ bit (for "must be zero") is currently unused and is either set to zero or just ignored.

0	1	2	3	4	5	6	7
Precedence			TOS				MBZ

IPv4 Packet Header Type of Service Octet

The four TOS bits provide 15 different priority values, however only five values have a defined meaning.

DiffServ Code Point (DSCP) — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network. DSCP are defined in RFC2597 for classifying traffic into different service classes. The IP DSLAM extracts the code point value of the DS field from IPv4 packets and identifies the priority of the incoming IP packets based on the configured priority.

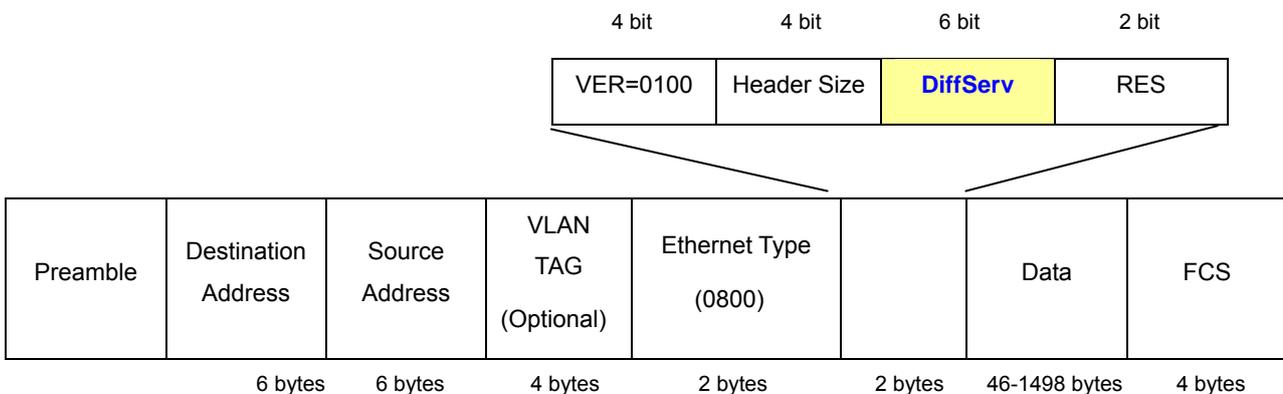


Figure 4-15-4: IPv4 frame format

The DSCP is **six bits** wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant, TOS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

4.15.3.1 TOS/DSCP Configuration

The **TOS/DSCP** page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the IP DSLAM recognizes TCP/IP Differentiated Service Code point (DSCP) priority information from the DS-field defined in RFC2474.

Enable TOS/DSCP for traffic classification and then the DSCP to priority mapping column is configurable, as the [Figure 4-15-5](#) shows:

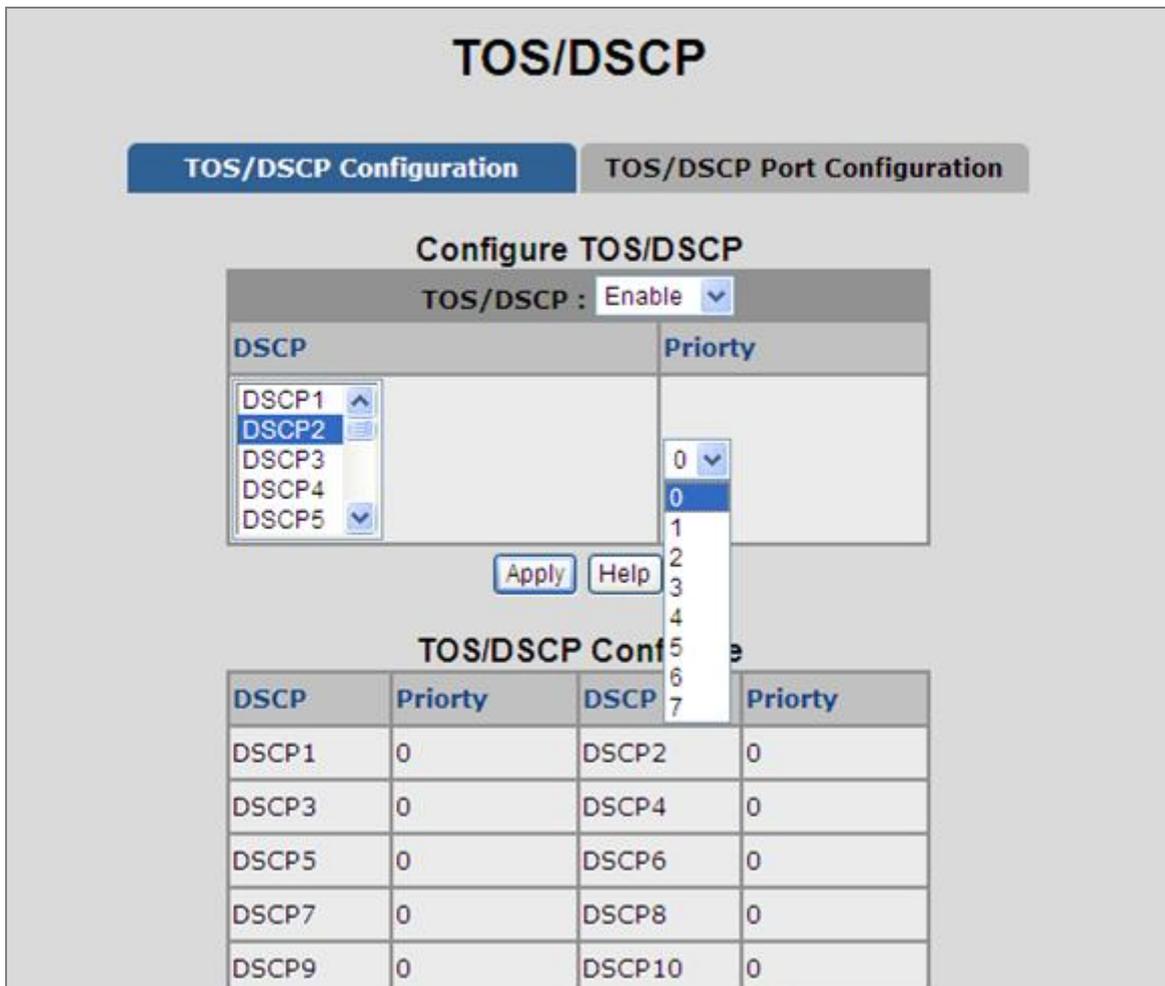


Figure 4-15-5: QoS Configuration – TOS Priority

The page includes the following fields:

Object	Description
TOS/DSCP	Enable / Disable internal traffic class (0~7) to map the corresponding IP DSCP value.
DSCP	The values of the IP DSCP header field within the incoming packet. 0~63.
Priority	Specify which 802.1p priority to map the corresponding IP DSCP. The value is 0~7.

4.15.3.2 TOS/DSCP Port Configuration

Set up IP TOS / DSCP mapping to 802.1p priority when receiving IPv4 packets, the IP DSLAM allow to by port configuring the QoS Status. This TOS/DSCP Port Configuration page is to configure the IP TOS/DSCP mapping on the port and display the current port status. The screen in [Figure 4-15-6](#) appears.

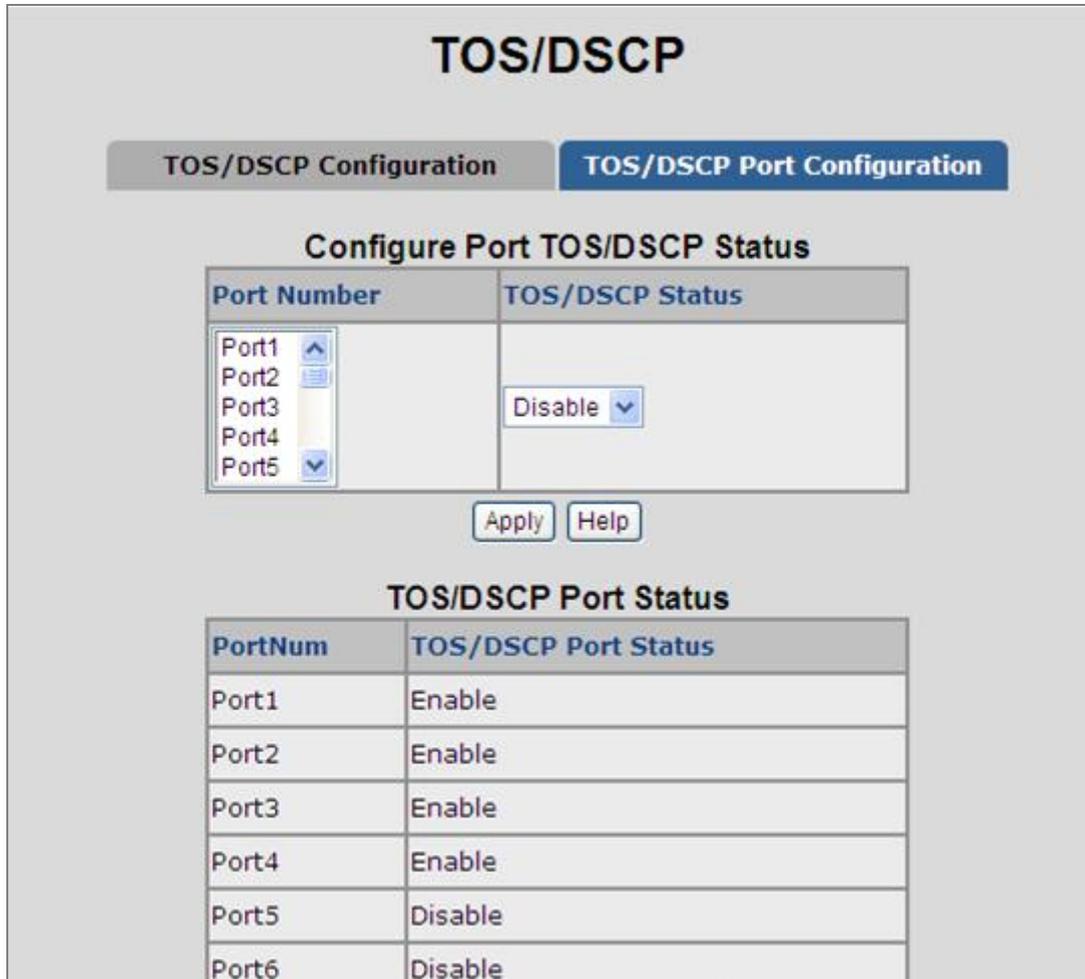


Figure 4-15-6: QoS Configuration – TOS/DSCP Port Status

The table includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 10.
TOS/DSCP Status	Enable / Disable TOS/DSCP map to 802.1p priority on specify port.

4.16 VDSL Configuration

VDSL2 (Very High-Bit-Rate Digital Subscriber Line 2), G.993.2 is the newest and most advanced standard of xDSL broadband wire line communications. Designed to support the wide deployment of Triple Play services such as voice, data, high definition television (HDTV) and interactive gaming, VDSL2 enable operators and carrier to gradually, flexibly, and cost efficiently upgrade exiting xDSL-infrastructure.

VDSL2 was developed and standardized in record time to address the shortcomings of existing access technologies. It servers as the ideal xDSL technology for eliminating last-mile bottlenecks and enable global mass deployment of advance Triple Play services. Unlike its predecessor, which allowed choosing either **DMT (Discrete Multitone)** or QAM (Quadrature Amplitude Modulation) technology, VDSL2 only uses the DMT line code.

DMT is a method of separating a DSL signal so that the usable frequency range is separated into multiple small frequency bands, or tone. It uses up to 4096 tones which are spaced 4 kHz or 8 kHz apart. Each tone can be used for either downstream or upstream.

The PLANET IP DSLAM can provide very high performance access to remote CPE, both downstream and upstream up to 100Mbps. The IP DSLAM complies with ITU-T G993.2 standard, and supports CO operating mode. The CO by WEB UI and users can connect to multiple CPE for Point-to-Multi-Point Application, data transmission between multiple networks over existing copper telephone lines.

4.16.1 Profile Management

As a managed node can handle a large number of CPE, (e.g., hundreds or perhaps thousands of lines), provisioning every parameter on every CPE may become burdensome. A profile is a set of parameters that can be shared by multiple lines using the same configuration.

The following profiles are used:

- **Line Configuration Profiles** - Line configuration profiles contain parameters for configuring VDSL lines. They are defined in the vdsLineConfProfileTable.
- **Alarm Configuration Profiles** - These profiles contain parameters for configuring alarm thresholds for VDSL transceivers. These profiles are defined in the vdsLineAlarmConfProfileTable.

One or more lines may be configured to share parameters of a single profile by setting their vdsLineConfProfile objects to the value of this profile. If a change is made to the profile, all lines that refer to it will be reconfigured to the changed parameters. Before a profile can be deleted or taken out of service it must be first unreferenced from all associated lines.

Implementations **MUST** provide a default profile with an index value of 'DEFVAL' for each profile type. Before a line's profiles have been set, these profiles will be automatically used by default profile. This default profile name, 'DEFVAL', is considered reserved in the context of profiles defined in system.

Profile changes **MUST** take effect immediately. These changes **MAY** result in a restart (hard reset or soft restart) of the units on the line.

4.16.1.1 Line Template

The Line Template provides user custom a line template name, and could choice the line profile and the channel profile what they want, and then bind with port. The screen in [Figure 4-16-1](#) appears.

Line Template

Line Template Name	<input type="text" value="user1"/>
Line Profile	<input type="text" value="user1"/> ▼
Channel Profile	<input type="text" value="user1"/> ▼

Line Template Name	Line Profile	Channel Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-1: Line Template Configuration

The table includes the following fields:

Object	Description
Line Template Name	Allows user to input the name of VDSL Line template.
Line Profile	Allows user to select Line profile.
Channel Profile	Allows user to select Channel profile.
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.1.2 Line Profile

This option allows to setup VDSL line configuration Profile. The screen in [Figure 4-16-2](#) appears.

Line Profile

Line Profile Name	<input type="text" value="DEFVAL"/>																
VDSL2 Profile	<input checked="" type="checkbox"/> 8a <input checked="" type="checkbox"/> 8b <input checked="" type="checkbox"/> 8c <input checked="" type="checkbox"/> 8d <input checked="" type="checkbox"/> 12a <input checked="" type="checkbox"/> 12b <input checked="" type="checkbox"/> 17a <input checked="" type="checkbox"/> 30a																
Band Profile	<input type="text" value="A_R_POTS_D-32_EU-32"/>																
Custom PSD Mask	<input type="text" value="DEFVAL"/>																
G.hs Carrier Set	<input checked="" type="radio"/> Auto <input type="radio"/> A43 <input type="radio"/> B43 <input type="radio"/> V43																
Allow USO	<input checked="" type="radio"/> Yes <input type="radio"/> No																
UPBO(Upstream Power Back-Off)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																
		<table border="1" style="width: 100%; text-align: center;"> <tr> <td></td> <td>US0</td> <td>US1</td> <td>US2</td> <td>US3</td> </tr> <tr> <td>Band A</td> <td><input type="text" value="4000"/></td> <td><input type="text" value="4000"/></td> <td><input type="text" value="4000"/></td> <td><input type="text" value="4000"/></td> </tr> <tr> <td>Band B</td> <td><input type="text" value="0"/></td> <td><input type="text" value="0"/></td> <td><input type="text" value="0"/></td> <td><input type="text" value="0"/></td> </tr> </table>		US0	US1	US2	US3	Band A	<input type="text" value="4000"/>	<input type="text" value="4000"/>	<input type="text" value="4000"/>	<input type="text" value="4000"/>	Band B	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
		US0	US1	US2	US3												
Band A	<input type="text" value="4000"/>	<input type="text" value="4000"/>	<input type="text" value="4000"/>	<input type="text" value="4000"/>													
Band B	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>													
	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																
DPBO(Downstream Power Back-Off)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																
	EsEL: <input type="text" value="0"/> 0.5dB	FMax: <input type="text" value="512"/> 4.1325kHz	FMin: <input type="text" value="32"/> 4.1325kHz														
	Mus: <input type="text" value="0"/> -0.5dB	DPBO PSD: <input type="text" value="DEFVAL"/>															
	ESCMA: <input type="text" value="0"/>	ESCMB: <input type="text" value="0"/>	ESCMC: <input type="text" value="0"/>														
SNR Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Virtual Noise PSD <input type="text" value="DEFVAL"/>																
RFI Band	<input type="text" value="DEFVAL"/>																
	Downstream	Upstream															
Target SNR	<input type="text" value="60"/> 0.1dB	<input type="text" value="60"/> 0.1dB															
Max Aggregate Transmit Power	<input type="text" value="145"/> 0.1dBm	<input type="text" value="145"/> 0.1dBm															
Max Transmit PSD	<input type="text" value="-365"/> 0.1dBm/Hz	<input type="text" value="-345"/> 0.1dBm/Hz															
Bitswap	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																
Rate Adaptation Mode	<input type="radio"/> Manual <input checked="" type="radio"/> RaInit <input type="radio"/> Dynamic																
	Up Shift SNR Margin	<input type="text" value="100"/> 0.1dB															
	Up Shift Time	<input type="text" value="3600"/> seconds															
	Down Shift SNR Margin	<input type="text" value="80"/> 0.1dB															
	Down Shift Time	<input type="text" value="3600"/> seconds															

Line Profile Name	VDSL2 Profile	Band Profile	Target SNR DS/US (0.1dB)	Applied Port
DEFVAL	30a,17a,12b,12a,8d,8c,8b,8a	A_R_POTS_D-32_EU-32	60/60	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	30a,17a,12b,12a,8d,8c,8b,8a	A_R_POTS_D-32_EU-32	60/60	

Figure 4-16-2: Line Profile Configuration

The table includes the following fields:

Object	Description
Line Profile Name	Allows inputting a custom Line profile name.
VDSL2 Profile	The VDSL2 The IP DSLAM provides most common VDSL2 profiles for user; it

	<p>supports the 30a, 17a, 12a, 12b, 8a, 8b, 8c and 8d. You can select the proper profile for your real environment.</p>
	<p>Different profiles provide different connection status of data rate and distance; please refer to Appendix A for more information.</p>
	<p>Click on the drop-down list and select the VDSL band plan to be used. The VDSL2 The IP DSLAM supports below profiles.</p>
<p>Band Profile</p>	<ol style="list-style-type: none"> 1. AnnexA_R_POTS_D-64_EU-64_30a 2. AnnexA_R_POTS_D-32_EU-32_17a 3. AnnexA_R_POTS_D-32_EU-32_12b 4. AnnexA_R_POTS_D-32_EU-32_12a 5. AnnexA_R_POTS_D-32_EU-32_8a 6. AnnexA_R_POTS_D-32_EU-32_8b 7. AnnexA_R_POTS_D-32_EU-32_8c 8. AnnexA_R_POTS_D-32_EU-32_8d 9. AnnexA_R_POTS_D-64_EU-64_30a_NUS0 10. AnnexA_R_POTS_D-64_EU-64_17^a 11. AnnexB_B7-1_997-M1c-A-7 12. AnnexB_B7-2_997-M1x-M-8 13. AnnexB_B7-3_997_M1x-M 14. AnnexB_B7-4_997_M2x-M-8 15. AnnexB_B7-5_997_M2x-A 16. AnnexB_B7-6_997_M2x-M 17. AnnexB_B7-9_997E17-M2x-A 18. AnnexB_B7-10_997E30-M2x-NUS0 19. AnnexB_B8-1_998-M1x-A 20. AnnexB_B8-2_998-M1x-B 21. AnnexB_B8-4_998-M2x-A 22. AnnexB_B8-5_998-M2x-M 23. AnnexB_B8-6_998-M2x-B 24. AnnexB_B8-8_998E17-M2x-NUS0 25. AnnexB_B8-9_998E17-M2x-NUS0-M 26. AnnexB_B8-10_998ADE17-M2x-NUS0-M 27. AnnexB_B8-11_998ADE17-M2x-A 28. AnnexB_B8-12_998ADE17-M2x-B 29. AnnexB_B8-13_998E30-M2x-NUS0 30. AnnexB_B8-14_998E30-M2x-NUS0-M 31. AnnexB_B8-15_998ADE30-M2x-NUS0-M 32. AnnexB_B8-16_998ADE30-M2x-NUS0-A 33. AnnexC_POTS_25-138_b 34. AnnexC_POTS_25-276_b 35. AnnexC_TCM-ISDN
<p>Custom PSD Mask</p>	<p>Power Spectral Density (PSD) mask code, used to avoid interference with HAM (Handheld Amateur Radio) radio bands by introducing power control (notching) in one or more of these bands. User could custom PSD Mask profile at Misc. Feature option.</p>
<p>G.hs Carrier Set</p>	<p>Allows set G.hs carrier. Default value is Auto.</p>
<p>Allow US0</p>	<p>Allows opening or closing US0. Default value is Yes.</p>

UPBO (Upstream Power-Back Off)	Upstream Power Back-off (UPBO) while received power exceeds configured max-aggregation-PSD in the upstream direction.
DPBO (Downstream Power Back-Off)	Downstream Power Back-off (DPBO) while received power exceeds configured max-aggregation-PSD in the downstream direction.
SNR Mode	Allows enabling or disabling SNR Mode.
Virtual Noise PSD	Allows simulating a virtual noise PSD profile which was set in Misc. Feature option.
RFI Band	Allows selecting a RFI Band profile which was set in Misc. Feature option.
Target SNR	<p>This is the Noise Margin the transceivers must achieve with a BER of 10^{-7} or better to successfully complete initialization.</p> <p>SNR margin value: 6 dB to 24 dB</p> <p>Default value: 6 dB (60 x 0.1 dB)</p>
Max. Aggregate Transmit Power	<p>Specifies the maximum downstream / upstream slow channel data rate in steps of 1000 bits/second. The maximum aggregate downstream transmit speed of the line can be derived from the sum of maximum downstream fast and slow channel data rates.</p>
Max. Transmit PSD	Allows inputting downstream / upstream transmit power spectral density.
Bitswap	<p>Allows enabling or disabling in downstream / upstream Bitswap.</p> <p>Once a transmission sub-channels affected by noise, it will transferred the bit to the signal quality of a good sub-channels.</p>
Rate Adaptation Mode	Allows
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.1.3 Channel Profile

The option allows user to configure Channel profile. The screen in Figure 4-16-3 appears.

Channel Profile

Channel Profile Name	<input type="text" value="DEFVAL"/>	
	Downstream	Upstream
Min Net Data Rate	<input type="text" value="256"/> kbps	<input type="text" value="256"/> kbps
Max Net Data Rate	<input type="text" value="101064"/> kbps	<input type="text" value="101064"/> kbps
Max Interleave Delay	<input type="text" value="8"/> ms	<input type="text" value="8"/> ms
Min INP for 30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols
Min INP for non-30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols

Channel Profile Name	Min Rate DS/US(kbps)	Max Rate DS/US (kbps)	Max Delay DS/US(ms)	Min INP for 30a Profile DS/US (symbols)	Min INP for non-30a Profile DS/US (symbols)	Applied Port
DEFVAL	256/256	101064/101064	8/8	2/2	2/2	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-3: Channel Profile Configuration

The table includes the following fields:

Object	Description
Channel profile Name	Allows inputting custom channel profile name.
Min Net Data Rate	Allows custom downstream / upstream minimal network data rate.
Max Net Data Rate	Allows custom downstream / upstream maximum network data rate.
Max Interleave Delay	Allows custom downstream / upstream maximum interleave delay.
Min INP for 30a Profile	Allows custom downstream / upstream minimal INP for 30a profile.
Min INP for non-30a Profile	Allows custom downstream / upstream minimal INP for non-30a profile.
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.1.4 Misc. Features

The option allows user to configure Virtual Noise PSD, RFI Band, DPBO PSD and Custom PSD Mask. The screen in [Figure 4-16-4](#) appears.

Misc. Features

Virtual Noise PSD
RFI Band
DPBO PSD
Custom PSD Mask

Virtual Noise PSD Name:

Downstream				Upstream			
Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)	Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)
1	<input type="text" value="1"/>	4.3	<input type="text" value="-140.0"/>	1	<input type="text" value="1"/>	4.3	<input type="text" value="-140.0"/>
2	<input type="text" value="31"/>	133.7	<input type="text" value="-140.0"/>	2	<input type="text" value="31"/>	133.7	<input type="text" value="-140.0"/>
3	<input type="text" value="32"/>	138.0	<input type="text" value="-120.0"/>	3	<input type="text" value="32"/>	138.0	<input type="text" value="-120.0"/>
4	<input type="text" value="6956"/>	29997.8	<input type="text" value="-120.0"/>	4	<input type="text" value="6956"/>	29997.8	<input type="text" value="-120.0"/>
5	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	5	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
6	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	6	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
7	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	7	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
8	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	8	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
9	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	9	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
10	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	10	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
11	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	11	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
12	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	12	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
13	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	13	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
14	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	14	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
15	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	15	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
16	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>	16	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>
17	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
18	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
19	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
20	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
21	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
22	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
23	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
24	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
25	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
26	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
27	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
28	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
29	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
30	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
31	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				
32	<input type="text" value="0"/>	0.0	<input type="text" value="0.0"/>				

Figure 4-16-4: Misc. Feature Configuration

4.16.1.4.1 Virtual Noise PSD

Virtual Noise OSD allows user custom a virtual noise for CPE before the CPE training. It could make CPE device adapt to bigger noise environment from beginning and avoid connection unstable or even connection is dropped in the future. The screen in Figure 4-16-5 appears.

Misc. Features

Virtual Noise PSD
RFI Band
DPBO PSD
Custom PSD Mask

Virtual Noise PSD Name:

Downstream				Upstream			
Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)	Break Point	Tone Index	Frequency (kHz)	Noise Level (dBm/Hz)
1	1	4.3	-140.0	1	1	4.3	-140.0
2	31	133.7	-140.0	2	31	133.7	-140.0
3	32	138.0	-120.0	3	32	138.0	-120.0
4	6956	29997.8	-120.0	4	6956	29997.8	-120.0
5	0	0.0	0.0	5	0	0.0	0.0
6	0	0.0	0.0	6	0	0.0	0.0
7	0	0.0	0.0	7	0	0.0	0.0
8	0	0.0	0.0	8	0	0.0	0.0
9	0	0.0	0.0	9	0	0.0	0.0
10	0	0.0	0.0	10	0	0.0	0.0
11	0	0.0	0.0	11	0	0.0	0.0
12	0	0.0	0.0	12	0	0.0	0.0
13	0	0.0	0.0	13	0	0.0	0.0
14	0	0.0	0.0	14	0	0.0	0.0
15	0	0.0	0.0	15	0	0.0	0.0
16	0	0.0	0.0	16	0	0.0	0.0
17	0	0.0	0.0				
18	0	0.0	0.0				
19	0	0.0	0.0				
20	0	0.0	0.0				
21	0	0.0	0.0				
22	0	0.0	0.0				
23	0	0.0	0.0				
24	0	0.0	0.0				
25	0	0.0	0.0				
26	0	0.0	0.0				
27	0	0.0	0.0				
28	0	0.0	0.0				
29	0	0.0	0.0				
30	0	0.0	0.0				
31	0	0.0	0.0				
32	0	0.0	0.0				

Edit and Add
Edit and Set
Delete
Clear

Virtual Noise PSD Name

[DEFVAL](#)

[CROSSTALK](#)

[VNS_WT115](#)

[user1](#)

[user2](#)

Figure 4-16-5: Virtual Noise PSD Configuration

The table includes the following fields:

Object	Description
Virtual Noise PSD Name	Allows to custom a virtual noise PSD profile.
Tone Index	Allows inputting Tone index number.
Noise Level (dB/Hz)	Allows inputting the tone frequency.
<input data-bbox="240 456 443 495" type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input data-bbox="240 510 443 548" type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input data-bbox="240 564 347 602" type="button" value="Delete"/>	Allows user to delete current line template.
<input data-bbox="240 618 331 656" type="button" value="Clear"/>	Recovery Table contents to default value.

4.16.1.4.2 RFI Band

RFI Band allows user to create RFI band frequency profile to avoid RFI band interference. The screen in [Figure 4-16-6](#) appears.

Misc. Features

Virtual Noise PSD
RFI Band
DPBO PSD
Custom PSD Mask

RFI Band Name:

Band Index	Start Tone	End Tone
1	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
2	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
3	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
4	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
5	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
6	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
7	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
8	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
9	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
10	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
11	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
12	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
13	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
14	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
15	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>
16	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>

Edit and Add
Edit and Set
Delete
Clear

Figure 4-16-6: RFI Band Configuration

The table includes the following fields:

Object	Description
RFI Band Name	Allows custom RFI Band profile name.
Start Tone	Allows inputting start tone number.
End Tone	Allows inputting end tone number.
Edit and Add	Allows user to create a new line template.
Edit and Set	Allows user to edit and save current line template.
Delete	Allows user to delete current line template.
Clear	Recovery Table contents to default value.

4.16.1.4.3 DPBO PSD

DPBO PSD allows user to create Downstream Power Back-Off PSD profile to avoid interference. The screen in [Figure 4-16-7](#) appears.

Misc. Features

Virtual Noise PSD
RFI Band
DPBO PSD
Custom PSD Mask

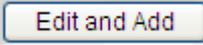
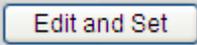
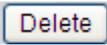
DPBO PSD Name:

Band Index	Tone	PSD Mask Level (dBm/Hz)
1	<input type="text" value="0"/>	<input type="text" value="-34.0"/>
2	<input type="text" value="6956"/>	<input type="text" value="-34.0"/>
3	<input type="text" value="0"/>	<input type="text" value="0.0"/>
4	<input type="text" value="0"/>	<input type="text" value="0.0"/>
5	<input type="text" value="0"/>	<input type="text" value="0.0"/>
6	<input type="text" value="0"/>	<input type="text" value="0.0"/>
7	<input type="text" value="0"/>	<input type="text" value="0.0"/>
8	<input type="text" value="0"/>	<input type="text" value="0.0"/>
9	<input type="text" value="0"/>	<input type="text" value="0.0"/>
10	<input type="text" value="0"/>	<input type="text" value="0.0"/>
11	<input type="text" value="0"/>	<input type="text" value="0.0"/>
12	<input type="text" value="0"/>	<input type="text" value="0.0"/>
13	<input type="text" value="0"/>	<input type="text" value="0.0"/>
14	<input type="text" value="0"/>	<input type="text" value="0.0"/>
15	<input type="text" value="0"/>	<input type="text" value="0.0"/>
16	<input type="text" value="0"/>	<input type="text" value="0.0"/>
17	<input type="text" value="0"/>	<input type="text" value="0.0"/>
18	<input type="text" value="0"/>	<input type="text" value="0.0"/>
19	<input type="text" value="0"/>	<input type="text" value="0.0"/>
20	<input type="text" value="0"/>	<input type="text" value="0.0"/>
21	<input type="text" value="0"/>	<input type="text" value="0.0"/>
22	<input type="text" value="0"/>	<input type="text" value="0.0"/>
23	<input type="text" value="0"/>	<input type="text" value="0.0"/>
24	<input type="text" value="0"/>	<input type="text" value="0.0"/>
25	<input type="text" value="0"/>	<input type="text" value="0.0"/>
26	<input type="text" value="0"/>	<input type="text" value="0.0"/>
27	<input type="text" value="0"/>	<input type="text" value="0.0"/>
28	<input type="text" value="0"/>	<input type="text" value="0.0"/>
29	<input type="text" value="0"/>	<input type="text" value="0.0"/>
30	<input type="text" value="0"/>	<input type="text" value="0.0"/>
31	<input type="text" value="0"/>	<input type="text" value="0.0"/>
32	<input type="text" value="0"/>	<input type="text" value="0.0"/>

Edit and Add
Edit and Set
Delete
Clear

Figure 4-16-7: DPBO PSD Configuration

The table includes the following fields:

Object	Description
DPBO PSD Name	Allows custom DPBO PSD profile name.
Tone	Allows inputting tone number.
PSD Mask Level (dB/Hz)	Allows inputting PSD mask level frequency.
	Allows user to create a new line template.
	Allows user to edit and save current line template.
	Allows user to delete current line template.
	Recovery Table contents to default value.

4.16.1.4.4 Custom PSD Mask

DPBO PSD allows user to create Downstream Power Back-Off PSD profile to avoid interference. The screen in [Figure 4-16-8](#) appears.

Misc. Features

Virtual Noise PSD
RFI Band
DPBO PSD
Custom PSD Mask

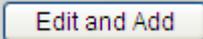
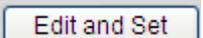
Custom PSD Mask Name:

Downstream				Upstream			
Break Point	Tone Index	Frequency (kHz)	PSD Mask Level (dBm/Hz)	Break Point	Tone Index	Frequency (kHz)	PSD Mask Level (dBm/Hz)
1	0	0.0	0.0	1	0	0.0	0.0
2	0	0.0	0.0	2	0	0.0	0.0
3	0	0.0	0.0	3	0	0.0	0.0
4	0	0.0	0.0	4	0	0.0	0.0
5	0	0.0	0.0	5	0	0.0	0.0
6	0	0.0	0.0	6	0	0.0	0.0
7	0	0.0	0.0	7	0	0.0	0.0
8	0	0.0	0.0	8	0	0.0	0.0
9	0	0.0	0.0	9	0	0.0	0.0
10	0	0.0	0.0	10	0	0.0	0.0
11	0	0.0	0.0	11	0	0.0	0.0
12	0	0.0	0.0	12	0	0.0	0.0
13	0	0.0	0.0	13	0	0.0	0.0
14	0	0.0	0.0	14	0	0.0	0.0
15	0	0.0	0.0	15	0	0.0	0.0
16	0	0.0	0.0	16	0	0.0	0.0
17	0	0.0	0.0	17	0	0.0	0.0
18	0	0.0	0.0	18	0	0.0	0.0
19	0	0.0	0.0	19	0	0.0	0.0
20	0	0.0	0.0	20	0	0.0	0.0
21	0	0.0	0.0	21	0	0.0	0.0
22	0	0.0	0.0	22	0	0.0	0.0
23	0	0.0	0.0	23	0	0.0	0.0
24	0	0.0	0.0	24	0	0.0	0.0
25	0	0.0	0.0	25	0	0.0	0.0
26	0	0.0	0.0	26	0	0.0	0.0
27	0	0.0	0.0	27	0	0.0	0.0
28	0	0.0	0.0	28	0	0.0	0.0
29	0	0.0	0.0	29	0	0.0	0.0
30	0	0.0	0.0	30	0	0.0	0.0
31	0	0.0	0.0	31	0	0.0	0.0
32	0	0.0	0.0	32	0	0.0	0.0
33	0	0.0	0.0	33	0	0.0	0.0
34	0	0.0	0.0	34	0	0.0	0.0
35	0	0.0	0.0	35	0	0.0	0.0
36	0	0.0	0.0	36	0	0.0	0.0
37	0	0.0	0.0	37	0	0.0	0.0
38	0	0.0	0.0	38	0	0.0	0.0
39	0	0.0	0.0	39	0	0.0	0.0
40	0	0.0	0.0	40	0	0.0	0.0

Edit and Add
Edit and Set
Delete
Clear

Figure 4-16-8: Custom PSD MASK Configuration

The table includes the following fields:

Object	Description
Custom PSD Mask Name	Allows custom PSD mask profile name.
Tone Index	Allows inputting tone number.
PSD Mask Level (dB/Hz)	Allows inputting PSD mask level frequency.
	Allows user to create a new line template.
	Allows user to edit and save current line template.
	Allows user to delete current line template.
	Recovery Table contents to default value.

4.16.1.5 Alarm Template

The Alarm Template provides user custom an alarm template name, and could choice the line alarm profile and the channel alarm profile what they want, and then bind with port.

Alarm Configuration Profiles contain parameters for configuring alarm thresholds for VDSL transceivers. The screen in [Figure 4-16-9](#) appears.

Alarm Template

Alarm Template Name	<input type="text" value="DEFVAL"/>
Line Alarm Profile	DEFVAL ▼
Channel Alarm Profile	DEFVAL ▼

Alarm Template Name	Line Alarm Profile	Channel Alarm Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	user1	user1	

Figure 4-16-9: Alarm Template Configuration

The table includes the following fields:

Object	Description
Alarm Template Name	Allows custom alarm template name.
Line Alarm Profile	Allows selecting line alarm profile.
Channel Alarm Profile	Allows selecting channel alarm profile.
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.1.6 Line Alarm Profile

DPBO PSD allows user to create Downstream Power Back-Off PSD profile to avoid interference. The screen in [Figure 4-16-10](#) appears.

Line Alarm Profile

Line Alarm Profile Name:

xtucFecs	<input type="text" value="0"/>	xturFecs	<input type="text" value="0"/>
xtucEs	<input type="text" value="0"/>	xturEs	<input type="text" value="0"/>
xtucSes	<input type="text" value="0"/>	xturSes	<input type="text" value="0"/>
xtucLoss	<input type="text" value="0"/>	xturLoss	<input type="text" value="0"/>
xtucUas	<input type="text" value="0"/>	xturUas	<input type="text" value="0"/>
FullInt	<input type="text" value="0"/>	ShrtInt	<input type="text" value="0"/>

Line Alarm Profile Name	xtucFecs	xtucEs	xtucSes	xtucLoss	xtucUas	xturFecs	xturEs	xturSes	xturLoss	xturUas	FullInt	ShrtInt	Applied Port
DEFVAL	0	0	0	0	0	0	0	0	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11
user1	0	0	0	0	0	0	0	0	0	0	0	0	12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-10: Line Alarm Profile Configuration

The table includes the following fields:

Object	Description
Line Alarm Profile Name	Allows user custom Line Alarm Profile name.
xtucFecs	Indicates that the FEC seconds threshold has been reached / exceeded for the referred xTU-C.
xtucEs	Indicates that the errored second threshold has been reached / exceeded for the referred xTU-C.
xtucSes	Indicates that the severely errored second threshold has been reached / exceeded for the referred xTU-C.
xtucLoss	Indicates that the LOS seconds threshold has been reached / exceeded for the referred xTU-C.
xtucUas	Indicates that the unavailable second threshold has been reached / exceeded for the referred xTU-C.
FullInt	Indicates that the failed full initializations threshold has been reached / exceeded for the referred VDSL2 line.
ShrtInt	Indicates that the failed short initializations threshold has been reached / exceeded for the referred VDSL2 line.
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.1.7 Line Alarm Profile

DPBO PSD allows user to create Downstream Power Back-Off PSD profile to avoid interference. The screen in [Figure 4-16-11](#) appears.

Channel Alarm Profile

Channel Alarm Profile Name:

	xtuc	xtur
cvThres	<input type="text" value="0"/>	<input type="text" value="0"/>
correctedThres	<input type="text" value="0"/>	<input type="text" value="0"/>

Channel Alarm Profile Name	cvThres.xtuc	correctedThres.xtuc	cvThres.xtur	correctedThres.xtur	Applied Port
DEFVAL	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11
user1	0	0	0	0	12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-11: Channel Alarm Profile Configuration

The table includes the following fields:

Object	Description
Channel Alarm Profile Name	Allows custom channel alarm profile name.
cvThres	Indicates that the coding violations threshold has been reached / exceeded for the referred xTU-C.
CorrectedThres	Indicates that the corrected blocks (FEC events) threshold has been reached/exceeded for the referred xTU-C.
<input type="button" value="Edit and Add"/>	Allows user to create a new line template.
<input type="button" value="Edit and Set"/>	Allows user to edit and save current line template.
<input type="button" value="Delete"/>	Allows user to delete current line template.

4.16.2 Port Management

The Port Management feature provides user binding port with line template and alarm template flexibility. Each of port could be selected different template.

4.16.2.1 Setup

This option provides user could change different template by port. The screen in [Figure 4-16-12](#) appears.

Port Setup

Port	Modify	Line Template	Alarm Template
1	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
2	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
3	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
4	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
5	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
6	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
7	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
8	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
9	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
10	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
11	<input type="checkbox"/>	DEFVAL ▼	DEFVAL ▼
12	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
13	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
14	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
15	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
16	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
17	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
18	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
19	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
20	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
21	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
22	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
23	<input type="checkbox"/>	DEFVAL ▼	user1 ▼
24	<input type="checkbox"/>	DEFVAL ▼	user1 ▼

Figure 4-16-12: Port Setup Configuration

The table includes the following fields:

Object	Description
Modify	Provides user to select which port wants to be changed template setting.
Line Template	Allows selecting line template profile.
Alarm Template	Allows selecting alarm template profile.
Modify All	Allows user to create a new line template.
Cancel All	Allows user to edit and save current line template.
Set	Allows user to delete current line template.

4.16.2.2 Status

This page provides all of VDSL port information. User can press Retrain button to retraining CPE device of remote or press Details button to view details VDSL connection information. The screen in [Figure 4-16-13](#) appears.

Port Status Refresh										
Port	Up Time(second)	Rate DS/US(kbps)	Status	INP DS/US(0.1 symbol)	Delay DS/US(ms)	CRC DS/US	Outbound Pkts	Inbound Pkts	Retrain	Details
1	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
2	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
3	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
4	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
5	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
6	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
7	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
8	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
9	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
10	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
11	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
12	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
13	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
14	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
15	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
16	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
17	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
18	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
19	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
20	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
21	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
22	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
23	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details
24	0	0/0	Idle	0/0	0/0	0/0	0	0	Retrain	Details

Figure 4-16-13: Port Status

The table includes the following fields:

Object	Description
Refresh	Allows user refresh Web page manually.
Retrain	Provides retraining CPE device of remote.
Details	Provides more details VDSL connection information.

The **Details** Button WEB page shows each of port details VDSL connection information. The screen in [Figure 4-16-14](#) appears.

Port Details

Port Number:

Port Info	
Items	Status
Port Number	1
Line Template	DEFVAL
Alarm Template	DEFVAL
Actual Profile	NA
Status	Idle
Firmware Version	131000

VDSL2 Status			
Items	Downstream	Upstream	Unit
Attainable Net Data Rate	0	0	kbps
Actual Net Data Rate	0	0	kbps
Previous Net Data Rate	0	0	kbps
Actual Delay	0	0	ms
Actual INP	0	0	0.1 symbol
SNR Margin	NA	NA	0.1 dB
Signal Attenuation	NA	NA	0.1 dB
Line Attenuation	NA	NA	0.1 dB
Electrical Length	0	0	0.1 dB
Actual Aggregate Transmit Power	0	0	0.1 dB
Trellis Coding	1	1	Enable(1)/Disable(0)
Interleave Depth	1	1	Counter
Interleave Block	4	4	Counter

VDSL2 Band Status	US	US0	US1	US2	US3	US4	DS	DS1	DS2	DS3	DS4	Unit
SNR Margin	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0.1 dB
Signal Attenuation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0.1 dB
Line Attenuation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	0.1 dB

VDSL2 PM Curr	Since Link		Curr 15 Min		Curr 1 Day	
	xtuc	xtur	xtuc	xtur	xtuc	xtur
Full Inits	-	-	0	-	0	-
Coding Violation	0	0	0	0	0	0
Corrected Blocks	0	0	0	0	0	0
Fecs	0	0	0	0	0	0
Es	0	0	0	0	0	0
Ses	0	0	0	0	0	0
Loss	0	0	0	0	0	0
Uas	2	0	413	0	2144	0
Time Elapsed	0	0	412	412	2212	2212

Figure 4-16-14: Port Details

The table includes the following fields:

Object	Description
Port Number	Allows user refresh Web page manually.
<input type="button" value="Query"/>	
<input type="button" value="Return"/>	

4.16.3 How to Setup VDSL

The Line template includes line profile and channel profile, so we have to configure them first and decides which wants be bind finally. However, there was a default setting exist in the system, in most case you could connect your CPE device to VDL-2420MR and it should be trained success.

Now, we have a situation. We need to prepare a Line template and the VDLS line setting is 30a profile, Annex A, downstream and upstream both 100Mbps then the template just only for port 1 and port 2.

4.16.3.1 Line Template and Profile Setup Example

Step1. Click **Line Profile** hyperlink on the menu of screen left. The screen in [Figure 4-16-15](#) appears.

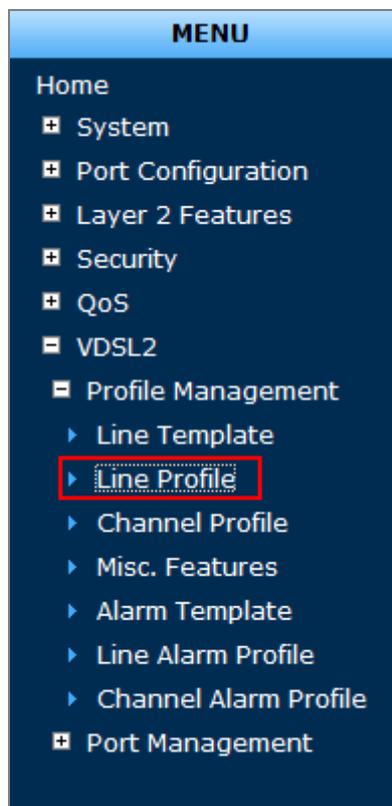


Figure 4-16-15: Port Details

Setp2. For this example we will create a user1 line profile with 30a, Annex A VDSL profile. Please rename the Line Profile Name because DEFVAL (default Value) can not be modified, and leave all VDSL2 profile blank but 30a and then choice A_R_POTS_D-32_EU-32 band profile. The First Letter A means Annex A and the first Letter B means Annex B. The screen in [Figure 4-16-16](#) appears.

The image shows a configuration form titled 'Line Profile'. It has three main sections: 'Line Profile Name' with a text input field containing 'user1'; 'VDSL2 Profile' with a row of radio buttons for profiles 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a, where the 30a option is selected; and 'Band Profile' with a dropdown menu showing 'A_R_POTS_D-32_EU-32'.

Figure 4-16-16: Line Profile Configuration

Step3. Please press Edit and Add button to create a new Line Profile. The screen in [Figure 4-16-17](#) appears.

Line Profile Name	VDSL2 Profile	Band Profile	Target SNR DS/US (0.1dB)	Applied Port
DEFVAL	30a,17a,12b,12a,8d,8c,8b,8a	A_R_POTS_D-32_EU-32	60/60	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	30a	A_R_POTS_D-32_EU-32	60/60	

Figure 4-16-17: Line Profile Configuration

Step4. Click **Channel Profile** hyperlink on the menu of screen left. The screen in [Figure 4-16-18](#) appears.

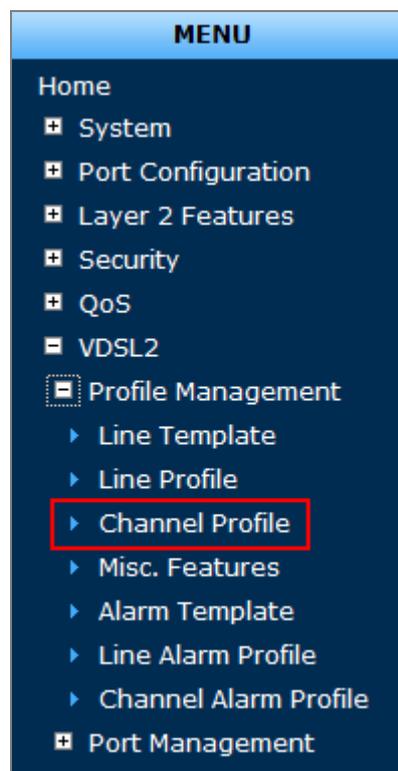


Figure 4-16-18: WEB UI management Menu

Step5. Rename DEFVAL to user1 at Channel profile Name. If you want limit downstream or upstream data rate, you can change them here. Per change range is 4Kbps. Please press **Edit and Add** button to create a new Channel profile. The screen in [Figure 4-16-19](#) and [Figure 4-16-20](#) appears.

Channel Profile

Channel Profile Name	<input type="text" value="user1"/>	
	Downstream	Upstream
Min Net Data Rate	<input type="text" value="258"/> kbps	<input type="text" value="256"/> kbps
Max Net Data Rate	<input type="text" value="101064"/> kbps	<input type="text" value="101064"/> kbps
Max Interleave Delay	<input type="text" value="8"/> ms	<input type="text" value="8"/> ms
Min INP for 30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols
Min INP for non-30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols
	<input type="button" value="Edit and Add"/>	<input type="button" value="Edit and Set"/> <input type="button" value="Delete"/>

Channel Profile Name	Min Rate DS/US(kbps)	Max Rate DS/US (kbps)	Max Delay DS/US(ms)	Min INP for 30a Profile DS/US (symbols)	Min INP for non-30a Profile DS/US (symbols)	Applied Port
DEFVAL	256/256	101064/101064	8/8	2/2	2/2	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-19: Channel Profile Configuration

Channel Profile

Channel Profile Name	<input type="text" value="user1"/>	
	Downstream	Upstream
Min Net Date Rate	<input type="text" value="258"/> kbps	<input type="text" value="256"/> kbps
Max Net Date Rate	<input type="text" value="101064"/> kbps	<input type="text" value="101064"/> kbps
Max Interleave Delay	<input type="text" value="8"/> ms	<input type="text" value="8"/> ms
Min INP for 30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols
Min INP for non-30a Profile	<input type="text" value="2"/> symbols	<input type="text" value="2"/> symbols
	<input type="button" value="Edit and Add"/>	<input type="button" value="Edit and Set"/> <input type="button" value="Delete"/>

Channel Profile Name	Min Rate DS/US(kbps)	Max Rate DS/US (kbps)	Max Delay DS/US(ms)	Min INP for 30a Profile DS/US (symbols)	Min INP for non-30a Profile DS/US (symbols)	Applied Port
DEFVAL	256/256	101064/101064	8/8	2/2	2/2	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	258/256	101064/101064	8/8	2/2	2/2	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-20: Channel Profile Configuration

Step6. Click **Channel Profile** hyperlink on the menu of screen left. The screen in [Figure 4-16-21](#) appears.

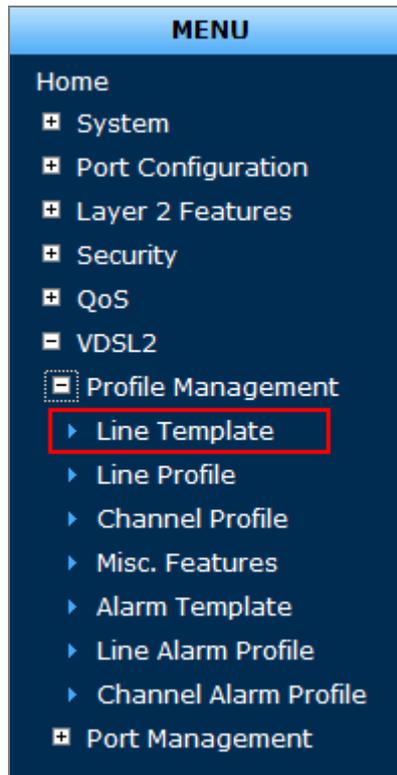


Figure 4-16-21: WEB UI management Menu

Step7. Please rename DEFVAL to user1 on Line Template name then select user1 on Line profile and Channel Profile, and then press **Edit and Add** button to create a new Line Template. The screen in Figure 4-16-22 and Figure 4-16-23 appears.

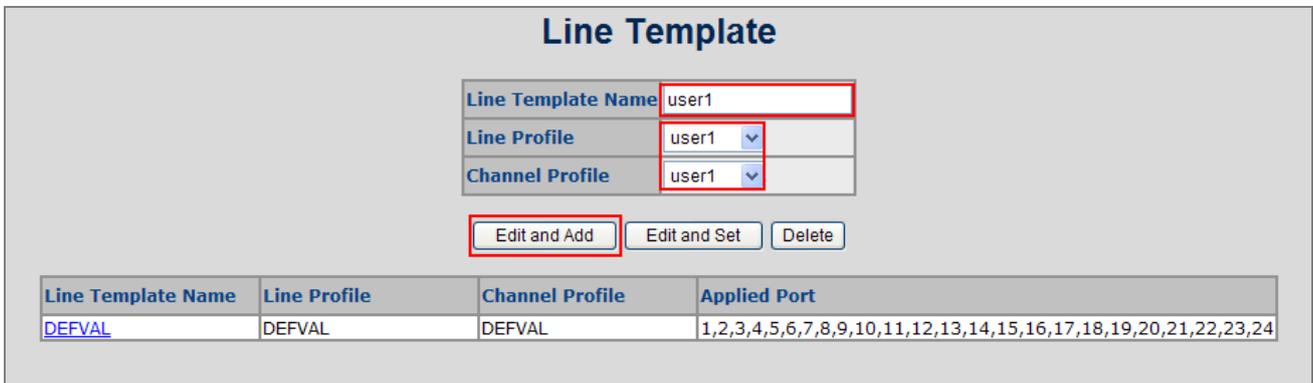


Figure 4-16-22: Line Template Configuration

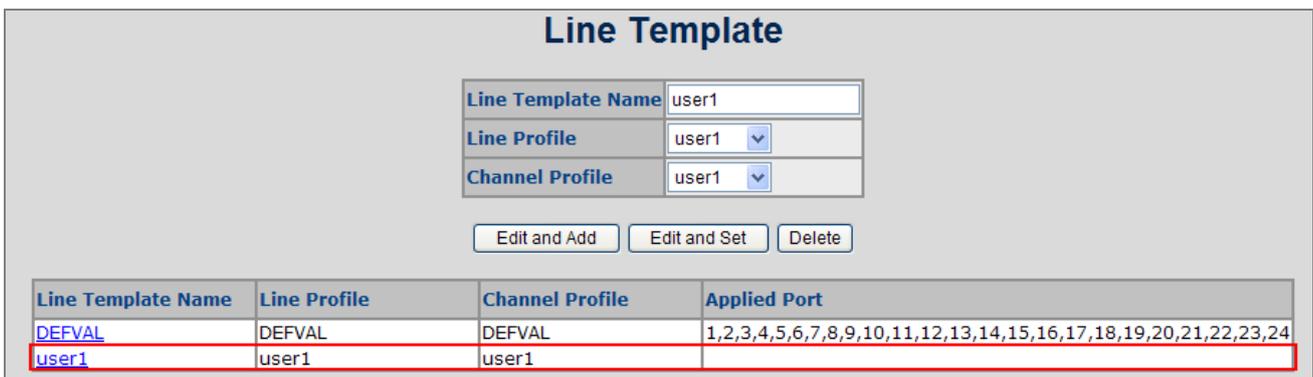


Figure 4-16-23: Line Template Configuration

4.16.3.2 Alarm Template and Profile Setup Example

Step1. Click **Line Alarm Profile** hyperlink on the menu of screen left. The screen in [Figure 4-16-24](#) appears.

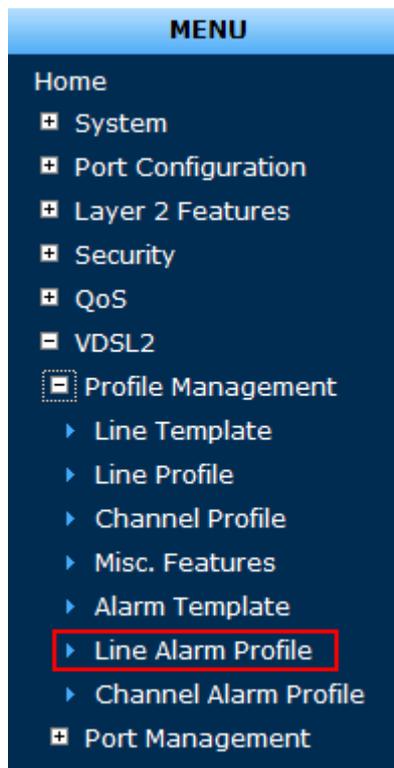


Figure 4-16-24: WEB UI management Menu

Step2. Rename DFEVAL to user1 on Line Alarm Profile Name and the press **Edit and Add** button to create a new profile. The screen in [Figure 4-16-25](#) and [Figure 4-16-26](#) appears.

Line Alarm Profile

Line Alarm Profile Name:

xtucFecs	<input type="text" value="0"/>	xturFecs	<input type="text" value="0"/>
xtucEs	<input type="text" value="0"/>	xturEs	<input type="text" value="0"/>
xtucSes	<input type="text" value="0"/>	xturSes	<input type="text" value="0"/>
xtucLoss	<input type="text" value="0"/>	xturLoss	<input type="text" value="0"/>
xtucUas	<input type="text" value="0"/>	xturUas	<input type="text" value="0"/>
FullInt	<input type="text" value="0"/>	ShrtInt	<input type="text" value="0"/>

Line Alarm Profile Name	xtucFecs	xtucEs	xtucSes	xtucLoss	xtucUas	xturFecs	xturEs	xturSes	xturLoss	xturUas	FullInt	ShrtInt	Applied Port
DEFVAL	0	0	0	0	0	0	0	0	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19

Figure 4-16-25: Line Alarm Profile Configuration

Line Alarm Profile

Line Alarm Profile Name:

xtucFecs	<input type="text" value="0"/>	xturFecs	<input type="text" value="0"/>
xtucEs	<input type="text" value="0"/>	xturEs	<input type="text" value="0"/>
xtucSes	<input type="text" value="0"/>	xturSes	<input type="text" value="0"/>
xtucLoss	<input type="text" value="0"/>	xturLoss	<input type="text" value="0"/>
xtucUas	<input type="text" value="0"/>	xturUas	<input type="text" value="0"/>
FullInt	<input type="text" value="0"/>	ShrtInt	<input type="text" value="0"/>

Line Alarm Profile Name	xtucFecs	xtucEs	xtucSes	xtucLoss	xtucUas	xturFecs	xturEs	xturSes	xturLoss	xturUas	FullInt	ShrtInt	Applied Port
DEFVAL	0	0	0	0	0	0	0	0	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22
user1	0	0	0	0	0	0	0	0	0	0	0	0	

Figure 4-16-26: Line Alarm Profile Configuration

Step3. Click **Channel Alarm Profile** hyperlink on the menu of screen left. The screen in [Figure 4-16-27](#) appears.

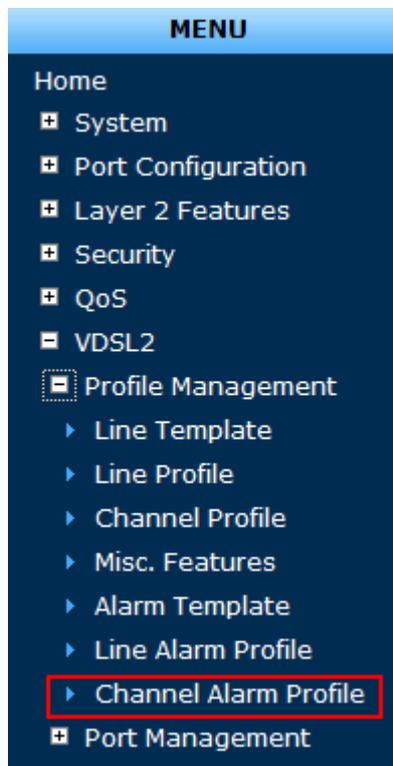


Figure 4-16-27: WEB UI management Menu

Step3. Rename DEFVAL to user1 on the Channel Alarm Profile name and then press **Edit and Add** button to create a new profile. The screen in [Figure 4-16-28](#) and [Figure 4-16-29](#) appears.

Channel Alarm Profile

Channel Alarm Profile Name:

	xtuc	xtur
cvThres	<input type="text" value="0"/>	<input type="text" value="0"/>
correctedThres	<input type="text" value="0"/>	<input type="text" value="0"/>

Channel Alarm Profile Name	cvThres.xtuc	correctedThres.xtuc	cvThres.xtur	correctedThres.xtur	Applied Port
DEFVAL	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-28: Channel Alarm Profile Configuration

Channel Alarm Profile

Channel Alarm Profile Name:

	xtuc	xtur
cvThres	<input type="text" value="0"/>	<input type="text" value="0"/>
correctedThres	<input type="text" value="0"/>	<input type="text" value="0"/>

Channel Alarm Profile Name	cvThres.xtuc	correctedThres.xtuc	cvThres.xtur	correctedThres.xtur	Applied Port
DEFVAL	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	0	0	0	0	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-29: Channel Alarm Profile Configuration

Step4. Click **Alarm Template** hyperlink on the menu of screen left. The screen in [Figure 4-16-30](#) appears.

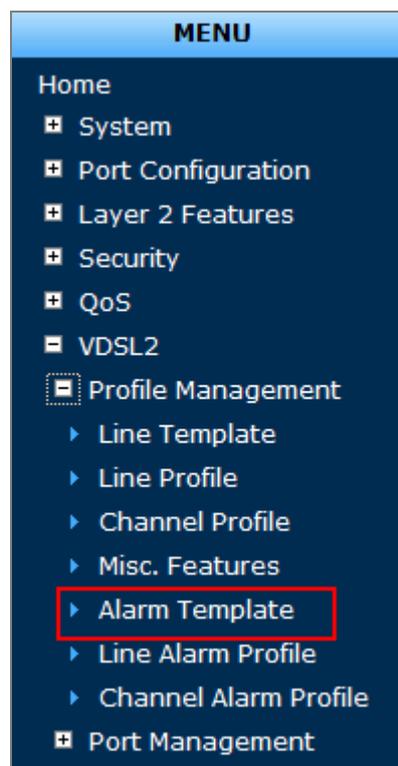


Figure 4-16-30: WEB UI management Menu

Step5. Rename DFEVAL to user1 on Alarm Template name then select both user1 on Line Alarm Profile and Channel Alarm Profile then press **Edit and Add** button to create a new template. The screen in [Figure 4-16-31](#) and [Figure 4-16-32](#) appears.

Alarm Template

Alarm Template Name	<input type="text" value="user1"/>
Line Alarm Profile	<input type="text" value="user1"/> ▼
Channel Alarm Profile	<input type="text" value="user1"/> ▼

Alarm Template Name	Line Alarm Profile	Channel Alarm Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Figure 4-16-31: Alarm Template Configuration

Alarm Template

Alarm Template Name	<input type="text" value="user1"/>
Line Alarm Profile	<input type="text" value="user1"/> ▼
Channel Alarm Profile	<input type="text" value="user1"/> ▼

Alarm Template Name	Line Alarm Profile	Channel Alarm Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	user1	user1	

Figure 4-16-32: Alarm Template Configuration

4.16.3.3 Port Setup Example

Until now, we have prepared profile but it still not is provided for connection with CPE device yet because the profile must be bind to interface port. Please follow the procedure as below to configure Port Setup.

Step1. Click **Setup** hyperlink on the menu of screen left. The screen in [Figure 4-16-33](#) appears.

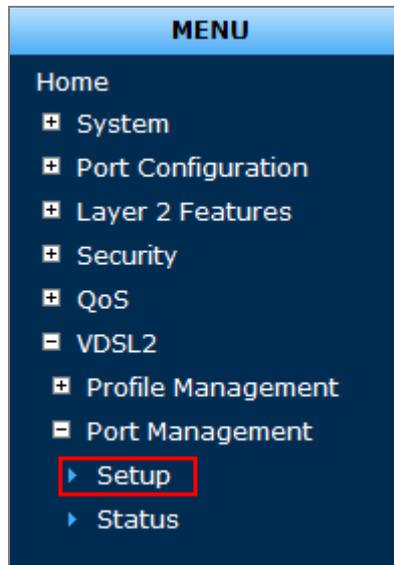


Figure 4-16-33: WEB UI management Menu

Step2. Checks Port 1 and Port2 checkbox at Modify field and then select user1 profile at Line Template and Alarm Template then press **Set** button to save this modifying. The screen in [Figure 4-16-34](#) appears.

Port	Modify	Line Template	Alarm Template
1	<input checked="" type="checkbox"/>	user1	user1
2	<input checked="" type="checkbox"/>	user1	user1
3	<input type="checkbox"/>	DEFVAL	DEFVAL
4	<input type="checkbox"/>	DEFVAL	DEFVAL
5	<input type="checkbox"/>	DEFVAL	DEFVAL
6	<input type="checkbox"/>	DEFVAL	DEFVAL
7	<input type="checkbox"/>	DEFVAL	DEFVAL
8	<input type="checkbox"/>	DEFVAL	DEFVAL
9	<input type="checkbox"/>	DEFVAL	DEFVAL
10	<input type="checkbox"/>	DEFVAL	DEFVAL

Figure 4-16-34 Port Setup

Step3. Then you will find Port1 and Port2 had been applied both on the Line Template and Alarm Template. The screen in Figure 4-16-35 and Figure 4-16-36 appears.

Line Template

Line Template Name	DEFVAL
Line Profile	DEFVAL
Channel Profile	DEFVAL

Line Template Name	Line Profile	Channel Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	user1	user1	1,2

Figure 4-16-35 Line Template Configuration

Alarm Template

Alarm Template Name	DEFVAL
Line Alarm Profile	DEFVAL
Channel Alarm Profile	DEFVAL

Alarm Template Name	Line Alarm Profile	Channel Alarm Profile	Applied Port
DEFVAL	DEFVAL	DEFVAL	3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
user1	user1	user1	1,2

Figure 4-16-36 Alarm Template Configuration

Step4. Now, you the Port 1 and Port 2 have been bind to user1 profile and you could connect to your CPE device and in joy the high speed network connection.

5. CONSOLE MANAGEMENT

The PLANET VDSL2 IP DSLAM series is equipped with a RS-232 DB9 connector as default. And both of the two models support telnet management.

5.1 Login in the Console Interface

To configure the system via console mode, connect a serial cable to a COM port on a PC or notebook computer and to RJ-45 type serial (console) port of the IP DSLAM. The console port of the IP DSLAM is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

Please refer to [chapter 3.5- Administration Console](#) to get more information about how to connect to the console interface of the IP DSLAM with HyperTerminal on Microsoft Windows platform.

Once the terminal has connected to the device, power on the IP DSLAM, the terminal will display that it is running testing procedures.

Then, the following message asks the login password. The factory default password as following and the login screen in [Figure 5-1-1](#) appears.

```
Username: admin
Password: admin
```

```
COM1_57600 HyperTerminal
File Edit View Call Transfer Help
portid=9,loid=2.1.30,value=3f3338
MIB value has set.
>>interface xdsl set oid 9 2.1.32 400010
portid=9,loid=2.1.32,value=400010
MIB value has set.
>># Setup Profile
>>interface xdsl set initprofile
Init port1 use profile name:default
Init port2 use profile name:default
Init port3 use profile name:default
Init port4 use profile name:default
Init port5 use profile name:default
Init port6 use profile name:default
Init port7 use profile name:default
Init port8 use profile name:default
Username: admin
Password:
Switch#
```

Connected 00:02:42 ANSIV 57600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 5-1-1: VDSL2 The IP DSLAM Console Login screen



- For security reason, please change and memorize the new username and password after this first setup.
Username Max: **6**, Min: **1** characters.
Password Max: **6**, Min: **1** characters.
- Only accept command in lowercase letter under console interface.

5.2 Configure IP address

The IP DSLAM is shipped with default IP address as following.

IP Address : **192.168.0.100**
Subnet Mask : **255.255.255.0**

To check the current IP address or modify a new IP address for the IP DSLAM, please use the procedures as follow:

■ Show the current IP address

- On "DSLAM#" prompt, enter "configure".
- On "DSLAM(config)#" prompt, enter "show ip".
- The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2-1.

```

COM1_57600 - HyperTerminal
File Edit View Call Transfer Help
QinQ.....OK
Forwarding.....OK
IP Mcst.....OK
IGMP.....OK
STP/RSTP/MSTP...OK
MIB.....OK
802.1X.....OK
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
Password:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# _

```

Figure 5-2-1: Show IP information screen

■ Configure IP address

1. On "DSLAM(config)#" prompt, enter the following command and press <Enter>. As show in Figure 5-2-2.

```
DSLAM(config)# ip address 192.168.1.100 255.255.255.0
DSLAM(config)# ip default-gateway 192.168.1.254
```

The previous command would apply the follow settings for the IP DSLAM.

IP: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254

```
COM1_57600 - HyperTerminal
File Edit View Call Transfer Help
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
assword:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
Switch(config)# show ip
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
Switch(config)# copy running-config startup-config
Switch(config)# _
```

Figure 5-2-2: Set IP address screen

2. Repeat Step 1 to check if the IP address is changed.

If the IP is successfully configured, the IP DSLAM will apply the new IP address setting immediately. You can access the Web interface of the IP DSLAM through the new IP address.



If you do not familiar with console command or the related parameter, enter "help" anytime in console to get the help description.

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

5.3 Commands Level

The following table lists the CLI commands and description.

Modes	Access Method	Prompt	Exit Method	About This Mode ¹
User EXEC	Begin a session with your DSLAM.	DSLAM>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to: <ul style="list-style-type: none"> • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	DSLAM#	Enter disable to exit.	The privileged command is the advanced mode. Use this mode to <ul style="list-style-type: none"> • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	DSLAM (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure those parameters that are going to be applied to your DSLAM.

6. COMMAND LINE INTERFACE

6.1 Operation Notice

To enter the "configuration" mode, you need to be in the privileged mode, and then types in the command **configure**:

```
DSLAM# configure
DSLAM (config) #
```

6.1.1. Command Line Editing

Keys Function

<Ctrl>-B	; ← Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command line.
<Ctrl>-F	; → Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N	; ↓ Enters the next command line in the command history.
<Ctrl>-P	; ↑ Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<Ctrl>	-W Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
	Delete the character at the cursor.

The following generic function keys provide functions in all of the menus:

6.1.2. Command Help

You may enter ? at any command mode, and the CLI will return possible commands at that point, along with some description of

6.2 System Commands

show running-config

Description:

Display the running configuration of the IP DSLAM.

copy running-config startup-config

Description:

Backup the IP DSLAM configurations.

erase startup-config

Description:

Reset to default factory settings at next boot time.

clear arp

Description:

<ip-addr> specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.

show arp

Description:

Show the IP ARP translation table.

ping

Description:

Send ICMP ECHO_REQUEST to network hosts.

Parameters:

<1..999> specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

syslog-server**Description:**

Set the syslog server information.

Syntax

syslog-server <IP address > [<0-2>]

Parameters:

<0-2 > specifies logging type. "0" is default value.

0: none

1: major

2: All

[no] sntp**Description:**

Enable / disable SNTP.

Syntax

[no] sntp

sntp**Description:**

Start SNTP service.

Syntax

sntp <IP address > [<Time Zone Offset>][<Time Range>]

Parameters:

<Time Zone Offset> specifies time zone offset is before / after UTC.

before-utc: Before-UTC

after-utc: After-UTC

<0-24 > Time range <Unit: hour>

6.3 DSLAM Static Configuration

6.3.1 Port Configuration and show status

port state

Turn the port state on or off.

Syntax:

port state <on | off> [<port-list>]

Parameters:

<port-list> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

port nego

Description:

Set port negotiation.

Syntax

port nego <force | auto | nway-force> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port speed

Description:

Set port speed (in mbps) and duplex.

Syntax:

port speed <10 | 100 | 1000> <full | half> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port flow

Description:

Enable or disable port flow control.

Syntax:

port flow <enable | disable> [<port-list>]

Parameters:

The <enable | disable> enables or disables flow control.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port rate

Description:

Set port effective ingress or egress rate.

Syntax:

```
port rate <ingress | egress> <0..8000> [<port-list>]
```

Parameters:

<0..8000> specifies the ingress or egress rate.<0..8000>

<port-list> specifies the ports to be set. If not entered, all ports are set.

port priority

Description:

Set port priority.

Syntax:

```
port priority <disable | 0..7> [<port-list>]
```

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port jumboframe

Description:

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

Syntax:

```
port jumboframe <enable | disable> [<port-list>]
```

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

show port status

Description:

Show port status, including port State, Link, Trunking, VLAN, Negotiation, Speed, Duplex, Flow control, Rate control ,Priority, Security, BSF control.

```
DSLAM(config)# show port status
```

```
-----  
Port 1 Information  
-----
```

```
State: on
```

```
Link: down
```

```
Trunking: none
```

```
VLAN: DEFAULT
```

```
Priority: disable
```

```
Security: off  
-----
```

```

Port 2 Information
-----
State: on
Link: down
Trunking: none
VLAN: DEFAULT
Priority: disable
Security: off
-----
Port 3 Information
-----
State: on
Link: down
--More--
    
```

show port statistics

Description:

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt, TxAbort, Collision, and DropPkt.

Parameters:

<port-id> specifies the port to be shown.

```

DSLAM(config)# show port statistics
-----
Port 1 Information
-----
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
Collision: 0
DropPkt: 0
-----
Port 2 Information
-----
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
Collision: 0
DropPkt: 0
-----
Port 3 Information
-----
--More--
    
```

show port protection

Description:

Show protected port information.

```
DSLAM(config)# show port protection
```

Port	Protected	Group
1	off	1
2	off	1
3	off	1
4	off	1
5	off	1
6	off	1
7	off	1
8	off	1
9	off	1
10	off	1
Trk1	off	1

6.4 Trunk Configuration

Trunk allows the IP DSLAM to combine ports so that they function like a single high-speed link. It can be used to increase the bandwidth to some devices to provide a high-speed link. For example, trunk is useful when making connections between switches or connecting servers to the IP DSLAM. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the IP DSLAM can balance the traffic among the remaining links.



1. The 10/100 Mbps port cannot be trunked with Gigabit port (Port 9 and Port 10).
2. All ports in the same trunk group will be treated as a single port. If a trunk group exists, the ports belonging to that trunk will be replaced by "TRUNK #" in the VLAN configuration screen. The following example configures Port 1~ Port 2 as "TRUNK 1."

6.4.1 Trunking Commands

show trunks

Description:

Show trunking information.

```
DSLAM(config)# show trunk
```

Group ID	LACP	Ports	LACP Active
1	Yes	1, 2	1, 2

trunk add

Description:

Add a new trunk group.

Syntax:

```
trunk add <trunk-id> <lacp / no-lacp> <port-list> <active-port-list>
```

Parameters:

<trunk-id> specifies the trunk group to be added.

<lacp / no-lacp> to specify the added trunk group to be LACP enabled

<port-list> specifies the ports to be set.

<active-port-list> specifies the ports to be set to LACP active.

no trunk

Description:

Delete an existing trunk group.

Syntax:

```
no trunk <trunk-id>
```

Parameters:

<trunk-id> specifies the trunk group to be deleted

6.4.2 LACP Command

[no] lacp

Description:

Enable/disable LACP.

lacp system-priority

Description:

Set LACP system priority.

Syntax:

lacp system-priority <1..65535>

Parameters:

<1..65535> specifies the LACP system priority.

no lacp system-priority

Description:

Set LACP system priority to the default value 32768.

show lacp status

Description:

Show LACP enable/disable status and system priority.

```
DSLAM(config)# show lacp status
LACP is enabled.
LACP system priority: 32768
```

show lacp

Description:

Show LACP information.

show lacp agg

Description:

Show LACP aggregator information.

Syntax:

show lacp agg <trunk-id>

Parameters:

<trunk-id> specifies the trunk group to be shown.

show lacp port

Description:

Show LACP information by port.

Syntax:

show lacp port <port-id>

Parameters:

<port-id> specifies the port to be shown.



If VLAN group exist, all of the members of static trunk group must be in same VLAN group.

6.5 VLAN Configuration

6.5.1 Virtual LANs

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a DSLAM is logically equivalent of reconnecting a group of network devices to another Layer 2 DSLAM. However, all the network devices are still plugged into the same DSLAM physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

The IP DSLAM supports two types of VLANs:

- **Port-based**
- **IEEE 802.1Q (tag) –based**

Only one of the two VLAN types can be enabled at one time.

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the IP DSLAM administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.

The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the IP DSLAMs can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1.

However, the IP DSLAM could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.

The IP DSLAM supports both Port-based VLAN and Tag-based (802.1Q) VLAN modes. The default configuration is

tag-based (802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the IP DSLAM belong to default VLAN, VID is 1.



You cannot delete the default VLAN group in 802.1Q VLAN mode.

6.5.2 VLAN Mode: Port-based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.



Change the VLAN mode for every time, user have to restart the IP DSLAM for valid value.

6.5.3 Advanced 802.1Q VLAN Configuration

Ingress filters configuration

When a packet was received on a port, you can govern the IP DSLAM to drop it or not if it is an untagged packet.

Furthermore, if the received packet is tagged but not belonging to the same VLAN group of the receiving port, you can also control the IP DSLAM to forward or drop the packet. The example below configures the IP DSLAM to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

VLAN Commands:

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.



Change the VLAN mode for every time, user have to restart the IP DSLAM for valid value.

vlan add

Description:

Add or edit VLAN entry.

Syntax:

vlan add <1-4094> NAME (cpu-port|no-cpu-port) LIST [LIST]

Parameters:

<1-4094> specifies the VLAN ID or Group ID (if port based VLAN mode)

NAME specifies the VLAN group name.

(cpu-port|no-cpu-port) specifies the CPU port belong this VLAN group.

LIST specifies the ports to be set to VLAN members.

[LIST] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

e.g.. DSLAM(config)# vlan add 1 vlan1 cpu-port 1-4

This VLAN entry has four members (from port1 to port4) and all members are untagged.

no vlan**Description:**

Delete VLAN entry.

Syntax:

no vlan <1-4094>

Parameters:

<1-4094> specifies the VLAN ID or group ID (if port based VLAN).

e.g. no vlan 1

show vlan**Description:**

Show VLAN entry information.

Syntax:

show vlan [<1-4094>]

Parameters:

<1-4094> specifies the VLAN ID, null means all valid entries.

e.g.

```

DSLAM(config)# show vlan 1
VLAN           : 1
Type           : Static
Creation Time (sec.): 43
CPU Port       : Yes

  Port | Member
-----+-----
  Port1 | Untagged
  Port2 | Untagged
  Port3 | Untagged
  Port4 | Untagged
  Port5 | Untagged
  Port6 | Untagged
  Port7 | Untagged
  Port8 | Untagged
  Port9 | Untagged
  Port10 | Untagged
  Trk1 | Untagged

```

show vlan static**Description:**

Show static VLAN entry information.

show vlan pvid**Description:**

Show port default VLAN ID.

Syntax:

show vlan pvid [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all port's PVID will be showed.

e.g.

```

DSLAM(config)# show vlan pvid
  Port | PVID
-----+-----
  Port1 | 1
  Port2 | 1
  Port3 | 1
  Port4 | 1
  Port5 | 1
  Port6 | 1
  Port7 | 1
  Port8 | 1
  Port9 | 1
  Port10 | 1
  Trk1 | 1

```

vlan filter

Description:

Set ingress filter rules.

Syntax:

vlan filter <enable | disable> <enable | disable> LIST

Parameters:

<enable | disable> specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

<enable | disable> specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.

show vlan filter

Description:

Show VLAN filter setting.

Syntax:

show vlan filter [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

```
DSLAM(config)# show vlan filter
```

```
Port | Rule 1 | Rule 2
Filter (nonmbr) (untag)
```

```
-----+-----+-----
Port1 | Drop   | Forward
Port2 | Drop   | Forward
Port3 | Drop   | Forward
Port4 | Drop   | Forward
Port5 | Drop   | Forward
Port6 | Drop   | Forward
Port7 | Drop   | Forward
Port8 | Drop   | Forward
Port9 | Drop   | Forward
Port10 | Drop  | Forward
Trk1 | Drop   | Forward
```

6.6 Misc Configuration

[no] mac-age-time

Description:

Disable MAC address age-out or set MAC address age-out time.

Syntax:

no mac-age-time Enable or disable MAC address age-out.

mac-age-time <6..1572858>

Parameters:

<6..1572858> specifies the MAC address age-out time. The MAC age-out time must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the IP DSLAM's address table.

show mac-age-time

Description:

Show MAC address age-out time

broadcast

Description:

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

Syntax:

broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16>

broadcast select

Description:

Select the Broadcast storm filter packet type:

- **Unicast/Multicast:** Flood unicast/multicast filter
- **Control Packets:** Control packets filter
- **IP multicast:** IP multicast packets filter
- **Broadcast Packets:** Broadcast Packets filter

Syntax:

broadcast select <unicast/multicast | control packet | ip-multicast | broadcast>

Collision-Retry

Description:

Collision-Retry setting

Syntax:

Collision-Retry <off | 16 | 32 | 48>

Parameters:

<16 | 32 | 48> – In Half-Duplex, collision-retry maximum is 16 (or 32, 48) times and packet will be dropped if collisions still happen

off – In Half-Duplex, if happen collision will retry forever (Default).

6.7 Administration Configuration

6.7.1 Change Username / Password

hostname

Description:

Set DSLAM name.

Syntax:

hostname <name-str>

Parameters:

<name-str> specifies the IP DSLAM name. If you would like to have spaces within the name, use quotes (“”) around the name.

no hostname

Reset the IP DSLAM name to factory default setting.

[no] password

Description:

Set or remove username and password for manager or operator.

Syntax:

[no] **password** <manager | operator | all>

Parameters:

The manager username and password is also used by the web UI.

6.7.2 IP Configuration

User can configure the IP setting and fill in the new value.

ip address

Description:

Set IP address and subnet mask.

Syntax:

```
ip address <ip-addr> <ip-mask>
```

ip default-gateway

Description:

Set the default gateway IP address.

Syntax:

```
ip default-gateway <ip-addr>
```

show ip

Description:

Show IP address, subnet mask, and the default gateway.

show info

Description:

Show basic information, including system info, MAC address, and versions.

```
DSLAM(config)# show info
Model name: VDL-2420MR
Description: 24-Port VDSL2 + 2G TP/SFP Combo IP DSLAM
MAC address: 00:30:4F:44:55:66
Firmware version: 1.08
CLI version: 1.07
802.1x: disabled
GVRP: disabled
LLDP: disabled
IGMP: enabled
LACP: enabled
```

dhcp

Description:

Set DSLAM as dhcp client, it can get IP from dhcp server.



If you set this command, the IP DSLAM will reboot.

show dhcp

Description:

show dhcp enable/disable.

6.7.3 Reboot DSLAM

boot

Description:

Reboot (warm-start) the IP DSLAM.

6.7.4 Reset to Default

erase startup-config

Description:

Reset configurations to default factory settings at next boot time.

6.7.5 TFTP Update Firmware

copy tftp firmware

Description:

Download firmware from TFTP server.

Syntax:

```
copy tftp firmware <ip-addr> <remote-file>
```

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

6.7.6 Restore Configure File

copy tftp <running-config | flash>

Description:

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword `running-config`.

If the remote file is the configuration flash image of the IP DSLAM instead, use the keyword `flash`.

Syntax:

```
copy tftp <running-config | flash> <ip-addr> <remote-file>
```

Parameters:

`<ip-addr>` specifies the IP address of the TFTP server.

`<remote-file>` specifies the file to be downloaded from the TFTP server.

6.7.7 Backup Configure File

copy <running-config | flash> tftp

Description:

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keyword `running-config`. If you want to save the configuration flash image instead, use the keyword `flash`.

Syntax:

```
copy <running-config | flash> tftp <ip-addr> <remote-file>
```

Parameters:

`<ip-addr>` specifies the IP address of the TFTP server.

6.8 MAC limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the IP DSLAM stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

User can configure the MAC limit setting and fill in the new value.

mac-limit

Description:

Enable MAC limit.

no mac-limit

Description:

Disable MAC limit.

mac-limit

Description:

Set port MAC limit value, 0 to turn off MAC limit of port.

Syntax:

Mac-limit <port-list> <1-64>

show mac-limit

Description:

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

6.9 Port Mirroring Configuration

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the IP DSLAM. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the IP DSLAM, you can specify one port to be the monitored ports and any single port to be the monitoring port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.



The default Port Monitoring setting is disabled.

mirror-port

Description:

Set port monitoring information. (RX only|TX only|both RX and TX)

Syntax:

mirror-port <rx | tx | both> <port-id> <port-list>

Parameters:

rx specifies monitoring rx only.

tx specifies monitoring tx only.

both specifies monitoring both rx and tx.

<port-id> specifies the analysis port ID. This port receives traffic from all monitored ports.

<port-list> specifies the monitored port list.

show mirror-port

Description:

Show port monitoring information

6.10 Quality of Service

There are four transmission queues with different priorities in the IP DSLAM: **Highest**, **SecHigh**, **SecLow** and **Lowest**. The IP DSLAM will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to "Disable", the IP DSLAM will not perform QoS on its switched network. If the QoS mode was set to "High Empty Then Low", the IP DSLAM will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to "**weight ratio**", the IP DSLAM will exhaust packets from the queues according to the ratio. The default value of QoS mode is "**weight 8:4:2:1**." That means the IP DSLAM will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the IP DSLAM received a packet, the IP DSLAM has to decide which queue to put the received packet into. In the IP DSLAM, it will put received packets into queues according to the settings of "802.1p Priority" and "Static Port Ingress Priority." When the received packet is an 802.1p tagged packet, the IP DSLAM will put the packet into a queue according to the 802.1p Priority setting.

Otherwise, the IP DSLAM will put the packet into a queue according the setting of Static Port Ingress Priority.

- **802.1p Priority:** the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The IP DSLAM can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.
- **Static Port Ingress Priority:** each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

6.10.1 QoS Configuration

QoS mode:

- **First Come First Service:** The sequence of packets sent is depending on arrive orders.
- **All High before Low:** The high priority packets sent before low priority packets.
- **WRR:** Weighted Round Robin. Select the preference given to packets in the IP DSLAM's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 second-high means that the IP DSLAM sends 8 highest-priority packets before sending 4 second-high priority packets.
- **Qos level:** 0~7 priority level can map to highest, second-high, second-low, lowest queue.

Commands:

qos priority

Description:

Set 802.1p priority.

Syntax:

qos priority <first-come-first-service | all-high-before-low |weighted-round-robin>

Parameters:

```
[<highest >][<sec-highweight>][<sec low -weight>] [<lowest-weight>]
```

e.g. qos priority weighted-round-robin 8,4,2,1

qos level**Description:**

Set priority levels to highest, second-high, second-low and lowest.

Syntax:

```
qos level < highest | second-high | second-low | lowest > <level-list>
```

Parameters:

<level-list> specifies the priority levels to be high or low.

Level must be between 0 and 7.

e.g. qos level highest 7

e.g. qos level lowest 0

show qos**Description:**

Show QoS configurations, including 802.1p priority, priority level.

e.g.

```
DSLAM(config)# show qos
QoS configurations:
QoS mode: weighted round robin
Highest weight: 8
Second High weight: 4
Second Low weight: 2
Lowest weight: 1
802.1p priority[0-7]:
Lowest   Lowest   SecLow   SecLow   SecHigh   SecHigh   Highest   Highest
```

6.10.2 Per Port Priority

port priority**Description:**

Set port priority.

Syntax:

```
port priority <disable | [0-7]> [<port-list>]
```

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

e.g. port priority disable 1-5

6.11 MAC Address Configuration

clear mac-address-table

Description:

Clear all dynamic MAC address table entries.

mac-address-table static

Description:

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

```
mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>
```

no mac-address-table static mac-addr

Description:

Delete static unicast or multicast MAC address table entries.

Syntax:

```
no mac-address-table static mac-addr <vlan-id>
```

show mac-address-table

Description:

Display MAC address table entries.

```
DSLAM(config)# show mac-address-table
```

MAC Address	VLAN	Type	Source
00:08:B6:00:06:90	1	Dynamic	9
00:40:63:00:65:30	1	Dynamic	Trk1
00:03:63:F7:80:7F	1	Dynamic	9

show mac-address table static

Description:

Display static MAC address table entries.

show mac-address-table multicast

Description:

Display multicast related MAC address table.

smac-address-table static

Description:

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

```
smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>
```

show smac-address-table

Description:

Display secondary MAC address table entries.

show smac-address-table multicast

Description:

Display multicast related secondary MAC address table.

[no] filter

Description:

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag matches the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

Syntax:

```
[no] filter <mac-addr> <vlan-id>
```

show filter

Description:

Display filter MAC address table.

6.12 STP/MSTP Commands

[no] spanning-tree

Description:

Enable or disable spanning-tree.

spanning-tree forward-delay

Description:

Set spanning tree forward delay of CIST, in seconds.

Syntax:

spanning-tree forward-delay <4-30>

Parameters:

<4-30> specifies the forward delay, in seconds. Default value is 15.



The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree hello-time

Description:

Set spanning tree hello time of CIST, in seconds.

Syntax:

spanning-tree hello-time <1-10>

Parameters:

<1-10> specifies the hello time, in seconds. Default value is 2.



The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree maximum-age

Description:

Set spanning tree maximum age of CIST, in seconds.

Syntax:

spanning-tree maximum-age <6-40>

Parameters:

<6-40> specifies the maximum age, in seconds. Default value is 20.



The parameters must enforce the following relationships:

$$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$$

spanning-tree priority

Description:

Set spanning tree bridge priority of CIST and all MSTIs.

Syntax:

spanning-tree priority <0-61440>

Parameters:

<0-61440> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

show spanning-tree

Description:

Show spanning-tree information.

show spanning-tree port

Description:

Show spanning tree per port information.

Syntax:

show spanning-tree port [<port-list>]

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

spanning-tree protocol-version

Description:

Change spanning tree protocol version of CIST.

Syntax:

spanning-tree protocol-version <stp | mstp>

Parameters:

stp specifies the original spanning tree protocol (**STP,802.1d**).

mstp specifies the multiple spanning tree protocol (**MSTP,802.1s**)

spanning-tree max-hops

Description:

Set spanning tree bridge maximum hops of CIST and all MSTIs.

Syntax:

spanning-tree max-hops <1-40>

Parameters:

<1-40> specifies the bridge maximum hops. Default value is **20**.

spanning-tree name**Description:**

Set spanning tree bridge name of CIST.

Syntax:

spanning-tree name [<name-string>]

Parameters:

<name-string> specifies the bridge name. Default name is null.

spanning-tree revision**Description:**

Set spanning tree bridge revision of CIST.

Syntax:

spanning-tree revision <0-65535>

Parameters:

<0-65535> specifies the bridge revision. Default value is 0.

spanning-tree port path-cost**Description:**

Set spanning tree port path cost of CIST.

Syntax:

spanning-tree port path-cost <1-200000000> [<port-list>]

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree port priority**Description:**

Set spanning tree port priority of CIST.

Syntax:

spanning-tree port priority <0-240> [<port-list>]

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port mcheck**Description:**

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

Syntax:

[no] spanning-tree port mcheck [*<port-list>*]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port**Description:**

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

Syntax:

[no] spanning-tree port edge-port [*<port-list>*]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp**Description:**

Disable or enable spanning tree protocol on the CIST port.

Syntax:

[no] spanning-tree port non-stp [*<port-list>*]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac**Description:**

Set the port of CIST to be point to point connection.

Syntax:

spanning-tree port point-to-point-mac *<auto | true | false>* [*<port-list>*]

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst**Description:**

Set spanning tree bridge priority of MSTI.

Syntax:

```
spanning-tree mst <0-15> priority <0-61440>
```

Parameters:

<0-15> specifies the MSTI instance ID.

<0-61440> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree mst <0-15> vlan [<vlan-list>]**Description:**

Set MSTI to map VLAN list.

Syntax:

```
spanning-tree mst <0-15> vlan [<vlan-list>]
```

Parameters:

<0-15> specifies the MSTI instance ID.

<vlan-list> specifies the mapped VLAN list. Null means all VLANs.

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]**Description:**

Set spanning tree port path cost of MSTI.

Syntax:

```
spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]
```

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> port priority <0-240> [<port-list>]**Description:**

Set spanning tree port priority of MSTI.

Syntax:

```
spanning-tree mst <0-15> port priority <0-240> [<port-list>]
```

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

no spanning-tree mst**Description:**

Delete the specific MSTI.

Syntax:

```
no spanning-tree mst <0-15>
```

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree

Description:

Show spanning-tree information of CIST.

show spanning-tree port

Description:

Show spanning tree port information of CIST.

Syntax:

```
show spanning-tree port [<port-list>]
```

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

show spanning-tree mst configuration

Description:

Show MST instance map.

Syntax:

```
show spanning-tree mst configuration
```

show spanning-tree mst <0-15>

Description:

Show MST instance information.

Syntax:

```
show spanning-tree mst <0-15>
```

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree mst <0-15> port <1-10>

Description:

Show specific port information of MST instance.

Syntax:

```
show spanning-tree mst <0-15> port <1-10>
```

Parameters:

<0-15> specifies the MSTI instance ID.

<1-10> specifies port number.

show vlan spanning-tree

Description:

Show per VLAN per port spanning tree status.

Syntax:

show vlan spanning-tree

6.13 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management the IP DSLAM.

6.13.1 System Options

[no] snmp

Description:

Enable or disable SNMP.

show snmp status

Description:

Show the enable or disable status of SNMP.

snmp system-name

Description:

Set agent system name string.

Syntax:

snmp system-name <name-str>

Parameters:

<name-str> specifies the system name string.

e.g. snmp system-name DSLAM

snmp system-location

Description:

Set agent location string.

Syntax:

snmp system-location <location-str>

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact

Description:

Set agent system contact string.

Syntax:

snmp system-contact <contact-str>

Parameters:

<contact-str> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Description:

Show SNMP system information.

6.13.2 Community Strings

snmp community

Description:

Set SNMP community string.

Syntax:

snmp community <read-sysinfo-only | read-all-only | read-write-all><community-str>

Parameters:

<community-str> specifies the community string.

e.g. snmp community read-all-only public

no snmp community

Description:

Delete SNMP community string.

Syntax:

no snmp community <community-str>

Parameters:

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Description:

Show SNMP community strings.

6.13.3 Trap Managers

snmp trap

Description:

Set SNMP trap receiver IP address, community string, and port number.

Syntax:

snmp trap <ip-addr> [<community-str>] [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<community-str> specifies the community string.

<1..65535> specifies the trap receiver port number. Default value is 162 if not specified.

e.g. snmp trap 192.168.200.1 public

no snmp trap**Description:**

Remove trap receiver IP address and port number.

Syntax:

no snmp trap <ip-addr> [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<1..65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap**Description:**

Show all trap receivers.

6.14 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

[no] igmp**Description:**

Enable/disable IGMP snooping.

Syntax:

[no] igmp

[no] igmp fastleave**Description:**

Enable/disable IGMP snooping fast leave. If enable, DSLAM will fast delete member who send leave report, else wait one sec.

Syntax:

[no] igmp fastleave

[no] igmp querier

Description:

Enable/disable IGMP snooping querier.

Syntax:

[no] igmp querier

[no] igmp CrossVLAN

Description:

Enable/disable IGMP snooping CrossVLAN

Syntax:

[no] igmp CrossVLAN

show igmp

Description:

Show IGMP snooping information.

Syntax:

show igmp <status | router | groups | table>

Parameters:

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Description:

Clear IGMP snooping statistics counters.

6.15 802.1x Protocol

[no] dot1x

Description:

Enable or disable 802.1x.

Syntax:

[no] dot1x

radius-server host

Description:

Set radius server IP, port number, and accounting port number.

Syntax:

radius-server host *<ip-addr>* *<1024..65535>* *<1024..65535>*

Parameters:

<ip-addr> specifies server's IP address.

The first *<1024..65535>* specifies the server port number.

The second *<1024..65535>* specifies the accounting port number.

radius-server key

Description:

Set 802.1x shared key.

Syntax:

radius-server key *<key-str>*

Parameters:

<key-str> specifies shared key string.

radius-server nas

Description:

Set 802.1x NAS identifier.

Syntax:

radius-server nas *<id-str>*

Parameters:

<id-str> specifies NAS identifier string.

show radius-server

Description:

Show radius server information, including radius server IP, port number, accounting port number, shared key, NAS identifier,

dot1x timeout quiet-period

Description:

Set 802.1x quiet period. (default: 60 seconds)

Syntax:

dot1x timeout quiet-period <10-65535>

Parameters:

<10-65535> specifies the quiet period, in seconds.

dot1x timeout tx-period

Description:

Set 802.1x Tx period. (default: 15 seconds).

Syntax:

dot1x timeout tx-period <10-65535>

Parameters:

<10-65535> specifies the Tx period, in seconds.

dot1x timeout supplicant

Description:

Set 802.1x supplicant timeout (default: 30 seconds)

Syntax:

dot1x timeout supplicant <10-300>

Parameters:

<10-300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server

Description:

Set radius server timeout (default: 30 seconds).

Syntax:

dot1x timeout radius-server <10-300>

Parameters:

<10-300> specifies the radius server timeout, in seconds.

dot1x max-req

Description:

Set 802.1x maximum request retries (default: 2 times).

Syntax:

dot1x max-req <1-10>

Parameters:

<1-10> specifies the maximum request retries.

dot1x timeout re-authperiod

Description:

Set 802.1x re-auth period (default: 3600 seconds).

Syntax:

```
dot1x timeout re-authperiod <30-65535>
```

Parameters:

<30-65535> specifies the re-auth period, in seconds.

show dot1x

Description:

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port

Description:

Set 802.1x per port information.

Syntax:

```
dot1x port <fu | fa | au | no> <port-list>
```

Parameters:

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<port-list> specifies the ports to be set.

show dot1x port

Description:

Show 802.1x per port information.

Syntax:

```
show dot1x port <port-list>
```

Parameters:

<port-list> specifies the ports to be set.

6.16 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The IP DSLAM can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on

6.16.1 IPv4 ACL commands

no acl

Description:

Delete ACL group.

Syntax:

no acl <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no acl 1

no acl count

Description:

Reset the ACL group count.

Syntax:

no acl count <Group ID>

Parameters:

Group ID: <1-220> specifies the group ID.

show acl

Description:

Show ACL group information.

Syntax:

show acl [<1-220>]

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g.

```
DSLAM(config)# show acl 1
Group Id : 1
-----
Action : Permit
Rules:
Vlan ID : Any
IP Fragement : Uncheck
Src IP Address : Any
Dst IP Address : Any
L4 Protocol : Any
```

```
Port ID : Any
Hit Octet Count : 165074
Hit Packet count : 472
```

acl (add|edit) <1-220> (permit|deny) <0-4094> ipv4 <0-255>

Description:

Add ACL group for IPv4.

Syntax:

```
acl add <1-220> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck)
<0-65535> <0-10>
```

Parameters:

<1-220> specifies the group ID.

(permit|deny) specifies the action. permit: permit packet cross DSLAM; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.

<0-10> specifies the Port ID. 0 means don't care.

e.g.

```
DSLAM(config)# acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0
```

This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN ID=1 and IPv4.

acl add <1-220> (qosvoip) <0-4094>

Description:

Add ACL group for IPv4.

Syntax:

```
acl add <1-220> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>
```

Parameters:

<1-220> specifies the group ID.

(qosvoip) specifies the action, do qos voip packet adjustment.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. `acl add 1 qosvoip 1 7 1 1 0 0 0 0 0`

6.16.2 Non-IPv4 ACL commands

`no acl <1-220>` and `show acl <1-220>` commands are same as IPv4 ACL commands.

`acl add <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>`

Description:

Add ACL group for non-IPv4.

Syntax:

`acl add <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>`

Parameters:

<1-220> specifies the group ID.

(permit|deny) specifies the action. permit: permit packet cross DSLAM; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-65535> specifies the Ether Type. 0 means don't care.

e.g. `acl add 1 deny 0 nonipv4 2054`. This ACL rule will drop all packets for ether type is 0x0806 and non-IPv4.

6.17 Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross DSLAM if all conditions match.

6.17.1 SIP/SMAC binding commands

bind

Description:

Enable binding function.

no bind

Description:

Disable binding function.

Syntax:

```
no bind <1-220>
```

Parameters:

<1-220> specifies the group ID.

e.g. no bind 1

no bind

Description:

Delete Binding group.

Syntax:

```
no bind <1-220>
```

Parameters:

<1-220> specifies the group ID.

e.g. no bind 1

show bind

Description:

Show Binding group information.

Syntax:

```
show bind [<1-220>]
```

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g. show bind 1

bind add

Description:

Add Binding group.

Syntax:

```
bind add <1-220> A:B:C:D:E:F <0-4094> A.B.C.D <1-10>
```

Parameters:

<1-220> specifies the group ID.

A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN ID. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the IP Address.

<1-10> specifies the Port ID.

e.g.

```
DSLAM(config)# bind add 1 00:11:22:33:44:55 0 192.168.1.1 1
```

This Binding rule will permit all packet cross DSLAM from device's IP is 192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to DSLAM port ID=1.

6.18 DHCP Configuration

[no] dhcp-option82

Description:

Enable/disable dhcp-option82 function.

Syntax:

[no] dhcp-option82

dhcp-option82

Description:

Enable or disable dhcp-option82 port.

Syntax:

dhcp-option82 <enable | disable> [<port-list>]

Parameters:

The <enable | disable> enables or disables dhcp-option82 port.

<port-list> specifies the ports to be set. If not entered, all ports are set

[no] dhcp-relay

Description:

Enable/disable dhcp-relay function.

Syntax:

[no] dhcp-relay

dhcp-relay

Description:

Enable or disable dhcp-option82 port.

Syntax:

dhcp-option82 <enable | disable> [<port-list>] [<IP address>]

Parameters:

The <enable | disable> enables or disables dhcp-relay port.

<port-list> specifies the ports to be set. If not entered, all ports are set

<IP address> specifies the DHCP server IP address.

dhcp-router

Description:

Assign a port to connect a DHCP server in a domain.

Syntax:

dhcp-router [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set

6.19 VDSL2 Commands

Profile		
	line-template	Commands for xDSL line configuration template.
	line-profile	Commands for xDSL line configuration profile.
	chanprofile	xDSL channel configuration profile.
	alarm-template	xDSL alarm template.
	line-alarm-profile	xDSL line alarm profile.
	chan-alarm-profile	xDSL channel alarm profile.
	pre-define	xDSL pre-define configuration.
	port	xDSL port configuration.
	chan-profile	Commands for xDSL channel configuration profile.

6.19.1 VDSL2 interface Commands

profile line-template

Description:

Commands for xDSL line configuration template.

Syntax:

profile line-template [new | del | set | show]

profile line-template new

Description:

Create new xDSL line configuration template.

Syntax:

Profile line-template new <name >

Parameters:

<NAME> Profile name

profile line-template del

Description:

Delete xDSL line configuration template.

Syntax:

Profile line-template del <Name >

Parameters:

<NAME> Profile name

profile line-template set

Description:

Set xdsl template profile.

Syntax:

Profile line-template set <line-profile | chan-profile> <TEMPNAME> <NAME>

Parameters:

<line-profile> Specifies the line configuration profile.

<chan-profile> Specifies the channel configuration profile.

<TEMPNAME> LineTemplate profile_name.

<NAME> LineProfile profile_name.

profile line-template show

Description:

Show all profile names or show detail information of a specified profile.

Syntax:

Profile line-template show

profile line-template show sprofile

Description:

Show system profile names.

Syntax:

Profile line-template show sprofile

```
Switch(config)# profile line-template show sprofile
CO_Default
CPE_Default
A_R_POTS_D-32_EU-32
A_R_POTS_D-64_EU-64
B7-1_997-M1c-A-7
B7-2_997-M1x-M-8
B7-3_997-M1x-M
B7-4_997-M2x-M-8
B7-5_997-M2x-A
B7-6_997-M2x-M
B7-7_HPE17-M1-NUS0
B7-8_HPE30-M1-NUS0
B7-9_997E17-M2x-A
B7-10_997E30-M2x-NUS0
B8-1_998-M1x-A
B8-2_998-M1x-B
```

```

B8-3_998-M1x-NUS0
B8-4_998-M2x-A
B8-5_998-M2x-M
B8-6_998-M2x-B
B8-7_998-M2x-NUS0
B8-8_998E17-M2x-NUS0
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#

```

profile line-template show line-template

Description:

Show line template names.

Syntax:

Profile line-template show line-template <NAME>

Parameters:

<Name> profile name

profile line-template show line-profile

Description:

Show line profile names.

Syntax:

Profile line-template show line-profile <NAME>

Parameters:

<Name> profile name

profile line-template show chan-profile

Description:

Show channel profile names.

Syntax:

Profile line-template show chan -profile <NAME>

Parameters:

<Name> profile name

profile line-template show alarm-template

Description:

Show line template names.

Syntax:

Profile line-template show alarm-template <NAME>

Parameters:

<Name> profile name

profile line-template show line-alarm-profile

Description:

Show line profile names.

Syntax:

Profile line-template show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile line-template show port

Description:

Show profile used in each port.

Syntax:

Profile line-template show port

profile line-template show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

Profile line-template show virtual-noise <NAME>

Parameters:

<Name> profile name

profile line-template show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

Profile line-template show dpbopsd <NAME>

Parameters:

<Name> profile name

profile line-template show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

Profile line-template show rfi-bands <NAME>

Parameters:

<Name> profile name

profile line-template show psd

Description:

Show single PsdMask line profile content.

Syntax:

Profile line-template show psd <NAME>

Parameters:

<Name> profile name

profile line-profile

Description:

Commands for xDSL line configuration profile.

Syntax:

```
profile line-profile [new | del | set | show]
```

profile line-profile new

Description:

Create new xDSL line configuration profile.

Syntax:

```
profile line-profile new <NAME>
```

Parameters:

<NAME> Profile name

profile line-profile del

Description:

Delete xDSL line configuration profile.

Syntax:

```
profile line-profile del <NAME>
```

Parameters:

<NAME> Profile name

profile line-profile show

Description:

Delete xDSL line configuration profile.

Syntax:

```
profile line-profile del <NAME>
```

Parameters:

<NAME> Profile name

profile line-profile show

Description:

Show all profile names or show detail information of a specified profile.

Syntax:

```
profile line-profile show
```

profile line-profile show sprofile**Description:**

Show system profile names.

Syntax:

profile line-profile show sprofile

```
Switch(config)# profile line-profile show sprofile
CO_Default
CPE_Default
A_R_POTS_D-32_EU-32
A_R_POTS_D-64_EU-64
B7-1_997-M1c-A-7
B7-2_997-M1x-M-8
B7-3_997-M1x-M
B7-4_997-M2x-M-8
B7-5_997-M2x-A
B7-6_997-M2x-M
B7-7_HPE17-M1-NUS0
B7-8_HPE30-M1-NUS0
B7-9_997E17-M2x-A
B7-10_997E30-M2x-NUS0
B8-1_998-M1x-A
B8-2_998-M1x-B
B8-3_998-M1x-NUS0
B8-4_998-M2x-A
B8-5_998-M2x-M
B8-6_998-M2x-B
B8-7_998-M2x-NUS0
B8-8_998E17-M2x-NUS0
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
```

```
DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#
```

profile line-profile show line-profile

Description:

Show line profile names.

Syntax:

```
profile line-profile show line-profile <NAME>
```

Parameters:

<Name> profile name

profile line-profile show chan-profile

Description:

Show channel profile names.

Syntax:

```
profile line-profile show chan-profile <NAME>
```

Parameters:

<Name> profile name

profile line-profile show alarm-template

Description:

Show alarm template names.

Syntax:

```
profile line-profile show alarm-template <NAME>
```

Parameters:

<Name> profile name

profile line-profile show line-alarm-profile

Description:

Show line alarm profile names.

Syntax:

profile line-profile show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile line-profile show port

Description:

Show profile used in each port.

Syntax:

profile line-profile show port

profile line-profile show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile line-profile show virtual-noise <NAME>

Parameters:

<Name> profile name

profile line-profile show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile line-profile show dpbopsd <NAME>

Parameters:

<Name> profile name

profile line-profile show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile line-profile show rfi-bands <NAME>

Parameters:

<Name> profile name

profile line-profile show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile line-profile show psd <NAME>

Parameters:

<Name> profile name

profile line-profile set

Description:

Set xDSL line configuration profile.

Syntax:

profile line-profile set

profile line-profile set sys

Description:

xDSL System profile.

Syntax:

profile line-profile set sys <NAME > <VALUE >

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set bnd

Description:

Band Profile name.

Syntax:

profile line-profile set bnd <NAME > <VALUE >

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set vns

Description:

Virtual Noise PSD Name.

Syntax:

profile line-profile set vns <NAME > <VALUE >

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set psd

Description:

PSD name.

Syntax:

profile line-profile set psd <NAME > <VALUE >

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set rfi

Description:

RFI name.

Syntax:

profile line-profile set rfi <NAME > <VALUE >

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set DPB

Description:

DpboEPsd name.

Syntax:

profile line-profile set DPB

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set profiles

Description:

xDSL Profiles,value is 8 bit bitmasks,0:non-active 1:active; bit7:30a,

Bit6:17a,Bit5:12b,Bit4:12a,Bit3:8d,Bit2:8c,Bit1:8b,Bit0:8a.

ex, active 30a value is 10000000.

Syntax:

```
profile line-profile set rfi <NAME > <VALUE >
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set targetSnrmDs

Description:

Signal Noise Ratio margin target at DS, value range 0~310.

Syntax:

```
profile line-profile set targetSnrmDs
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set targetSnrmUs

Description:

Signal Noise Ratio margin target at US, value range 0~310.

Syntax:

```
profile line-profile set targetSnrmUs
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxSnrmDs

Description:

Signal Noise Ratio margin max at DS, value range 0~310.

Syntax:

```
profile line-profile set maxSnrmDs
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxSnrmUs

Description:

Signal Noise Ratio margin max at US, value range 0~310.

Syntax:

profile line-profile set maxSnrmUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set minSnrmDs

Description:

Signal Noise Ratio margin min at DS, value range 0~310.

Syntax:

profile line-profile set minSnrmDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set minSnrmUs

Description:

Signal Noise Ratio margin min at US, value range 0~310.

Syntax:

profile line-profile set minSnrmUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set led

Description:

On/Off vdsl led slow flash of light at vdsl idle status, value is on or off.

Syntax:

profile line-profile set minSnrmUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set bitSwapUs

Description:

On/Off Upstream bit swapping, value is on or off.

Syntax:

profile line-profile set bitSwapUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set bitSwapDs

Description:

On/Off Downstream bit swapping, value is on or off.

Syntax:

profile line-profile set bitSwapDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set us0disable

Description:

Upstream band number 0, value is allow or disable.

Syntax:

profile line-profile set us0disable

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set handshakeTone

Description:

Handshake tone mode, value range is 0,1,2,7. 0: auto, 1:AnnxA, 2:AnnexB, 7:AnnexC.

Syntax:

profile line-profile set handshakeTone

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboKLF

Description:

UPBO force mode, value range is 1~3, 1:auto, 2:override, 3:disableUpbo.

Syntax:

profile line-profile set upboKLF

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdA0

Description:

UPBO Parameter A for band 0, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdA0

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdB0

Description:

UPBO Parameter B for band 0, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdB0

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdA1

Description:

UPBO Parameter A for band 1, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdA1

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdB1

Description:

UPBO Parameter B for band 1, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdB1

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdA2

Description:

UPBO Parameter A for band 2, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdA2

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdB2

Description:

UPBO Parameter B for band 2, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdB2

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdA3

Description:

UPBO Parameter A for band 3, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdA3

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set upboPsdB3

Description:

UPBO Parameter B for band 3, value range is 4000~8095.

Syntax:

profile line-profile set upboPsdB3

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboEsEL

Description:

The electrical length of exchange to cabinet cable, value range is 0~511.

Syntax:

profile line-profile set dpboEsEL

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboEsCableModelA

Description:

E-side cable model parameter A, value range is 0~640.

Syntax:

profile line-profile set dpboEsCableModelA

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboEsCableModelB

Description:

E-side cable model parameter B, value range is 0~640.

Syntax:

profile line-profile set dpboEsCableModelB

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboEsCableModelC

Description:

E-side cable model parameter C, value range is 0~640.

Syntax:

profile line-profile set dpboEsCableModelC

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboMus

Description:

Assumed minimum usable PSD mask of exchange signals at remote site, value range is 0~255.

Syntax:

profile line-profile set dpboMus

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set dpboFMin

Description:

The lower bound on the DPBO frequency span, value range is 0~2048.

Syntax:

profile line-profile set dpboFMin

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set bpboFMax

Description:

The upper bound on the DPBO frequency span, value range is 36~6956.

Syntax:

profile line-profile set bpboFMax

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raModeDs**Description:**

The mode of operation of a rate-adaptive xTU-C in the transmit direction, value is 1:manual, 2:raNit, 3:dynamicRa.

Syntax:

profile line-profile set raModeDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raModeUs**Description:**

The mode of operation of a rate-adaptive xTU-R in the transmit direction, value is 1:manual, 2:raNit, 3:dynamicRa.

Syntax:

profile line-profile set raModeUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raUsNrmDs**Description:**

Downstream up-shift Signal/Noise Margin, value range is 0~310.

Syntax:

profile line-profile set raUsNrmDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raUsNrmUs**Description:**

Upstream up-shift Signal/Noise Margin, value range is 0~310.

Syntax:

profile line-profile set raUsNrmUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raUsTimeDs

Description:

Downstream up-shift time interval, value range is 0~16383.

Syntax:

profile line-profile set raUsTimeDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set raUsTimeUs

Description:

Upstream down-shift time interval, value range is 0~16383.

Syntax:

profile line-profile set raUsTimeUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set snrModeDs

Description:

virtual noise is active on the line in the downstream, value is enable or disable.

Syntax:

profile line-profile set snrModeDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set snrModeUs

Description:

Virtual noise is active on the line in the upstream, value is enable or disable.

Syntax:

profile line-profile set snrModeUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxNomAtpDs

Description:

Maximum nominal aggregate transmit power in the downstream, value range is -300~-600 units 0.1dBm/Hz.

Syntax:

profile line-profile set maxNomAtpDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxNomAtpUs

Description:

Maximum nominal aggregate transmit power in the upstream, value range is -300~-600 units 0.1dBm/Hz.

Syntax:

profile line-profile set maxNomAtpUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxNomPsdDs

Description:

Maximum nominal aggregate transmit PSD in the downstream, value range is -300~-600 units 0.1dBm/Hz.

Syntax:

profile line-profile set maxNomPsdDs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile line-profile set maxNomPsdUs

Description:

Maximum nominal aggregate transmit PSD in the upstream, value range is -300~-600 units 0.1dBm/Hz.

Syntax:

profile line-profile set maxNomPsdUs

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chanprofile

Description:

xDSL channel configuration profile.

Syntax:

profile chanprofile [show]

Parameters:

<show > Show all profile names or show detail information of a specified profile.

profile chanprofile show sprofile

Description:

Show system profile names.

Syntax:

profile show sprofile

profile chanprofile show line-template

Description:

Show line template names.

Syntax:

profile show line-template <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show line-profile

Description:

Show line profile names.

Syntax:

profile show line-profile <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show chan-profile

Description:

Show channel profile names.

Syntax:

profile show line-alarm-profile <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show alarm-template

Description:

Show line template names.

Syntax:

profile show alarm-template <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show line-alarm-profile

Description:

Show line profile names.

Syntax:

profile show line-alarm-profile <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show chan-alarm-profile

Description:

Show channel profile names.

Syntax:

profile show chan-alarm-profile <NAME>

Parameters:

<NAME> Profile name

profile chanprofile show port

Description:

Show profile used in each port.

Syntax:

profile show port

profile chanprofile show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile show virtual-noise

Parameters:

<NAME> Profile name

profile chanprofile show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile show dpbopsd

Parameters:

<NAME> Profile name

profile chanprofile show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile show rfi-bands

Parameters:

<NAME> Profile name

profile chanprofile show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile show psd

Parameters:

<NAME> Profile name

profile alarm-template

Description:

xDSL alarm template.

Syntax:

profile alarm-template [show | new | del | set]

Parameters:

<show> Show all profile names or show detail information of a specified profile.

<new> Create new xDSL alarm template.

 delete xDSL alarm template.

<set> set xDSL alarm template.

profile alarm-template show sprofile**Description:**

Show system profile names.

Syntax:

profile alarm-template show sprofile

```
Switch(config)# profile alarm-template show sprofile
CO_Default
CPE_Default
A_R_POTS_D-32_EU-32
A_R_POTS_D-64_EU-64
B7-1_997-M1c-A-7
B7-2_997-M1x-M-8
B7-3_997-M1x-M
B7-4_997-M2x-M-8
B7-5_997-M2x-A
B7-6_997-M2x-M
B7-7_HPE17-M1-NUS0
B7-8_HPE30-M1-NUS0
B7-9_997E17-M2x-A
B7-10_997E30-M2x-NUS0
B8-1_998-M1x-A
B8-2_998-M1x-B
B8-3_998-M1x-NUS0
B8-4_998-M2x-A
B8-5_998-M2x-M
B8-6_998-M2x-B
B8-7_998-M2x-NUS0
B8-8_998E17-M2x-NUS0
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
```

```

DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#

```

profile alarm-template show line-profile

Description:

Show line profile names.

Syntax:

```
profile alarm-template show line-profile <NAME>
```

Parameters:

<Name> profile name

profile alarm-template show chan-profile

Description:

Show channel profile names.

Syntax:

```
profile alarm-template show chan-profile <NAME>
```

Parameters:

<Name> profile name

profile alarm-template show alarm-template

Description:

Show alarm template names.

Syntax:

```
profile alarm-template show alarm-template <NAME>
```

Parameters:

<Name> profile name

profile alarm-templateshow line-alarm-profile

Description:

Show line alarm profile names.

Syntax:

profile alarm-template show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile alarm-template show port

Description:

Show profile used in each port.

Syntax:

profile alarm-template show port

profile alarm-template show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile alarm-template show virtual-noise <NAME>

Parameters:

<Name> profile name

profile alarm-template show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile alarm-template show dpbopsd <NAME>

Parameters:

<Name> profile name

profile alarm-template show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile alarm-template show rfi-bands <NAME>

Parameters:

<Name> profile name

profile alarm-template show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile alarm-template show psd <NAME>

Parameters:

<Name> profile name

profile alarm-template new

Description:

Create new xDSL alarm template.

Syntax:

profile alarm-template new <NAME>

Parameters:

<Name> profile name

profile alarm-template del

Description:

Delete xDSL alarm template.

Syntax:

profile alarm-template del <NAME>

Parameters:

<Name> profile name

profile alarm-template set line-alarm-profile

Description:

Specifies the line alarm configuration profile.

Syntax:

profile alarm-template set line-alarm-profile <TEMPNAME><NAME>

Parameters:

<TEMPNAME> AlarmTemplate profile_name.

<NAME> LineAlarmProfile profile_name

profile alarm-template set chan-alarm-profile

Description:

Specifies the channel alarm configuration profile.

Syntax:

```
profile alarm-template set chan-alarm-profile <TEMPNAME><NAME>
```

Parameters:

<TEMPNAME> AlarmTemplate profile_name.

<NAME> LineAlarmProfile profile_name

profile line-alarm-profile

Description:

xDSL line alarm profile.

Syntax:

```
profile line-alarm-profile [show | new | del | set]
```

Parameters:

<show> Show all profile names or show detail information of a specified profile.

<new> Create new xDSL alarm template.

 delete xDSL alarm template.

<set> set xDSL alarm template.

profile line-alarm-profile show sprofile

Description:

Show system profile names.

Syntax:

```
profile line-alarm-profile show sprofile
```

```
Switch(config)# profile line-alarm-profile show sprofile
CO_Default
CPE_Default
A_R_POTS_D-32_EU-32
A_R_POTS_D-64_EU-64
B7-1_997-M1c-A-7
B7-2_997-M1x-M-8
B7-3_997-M1x-M
B7-4_997-M2x-M-8
B7-5_997-M2x-A
B7-6_997-M2x-M
B7-7_HPE17-M1-NUS0
B7-8_HPE30-M1-NUS0
B7-9_997E17-M2x-A
```

B7-10_997E30-M2x-NUS0
B8-1_998-M1x-A
B8-2_998-M1x-B
B8-3_998-M1x-NUS0
B8-4_998-M2x-A
B8-5_998-M2x-M
B8-6_998-M2x-B
B8-7_998-M2x-NUS0
B8-8_998E17-M2x-NUS0
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#

profile line-alarm-profile show line-profile

Description:

Show line profile names.

Syntax:

profile line-alarm-profile show line-profile <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show chan-profile

Description:

Show channel profile names.

Syntax:

profile line-alarm-profile show chan-profile <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show alarm-template

Description:

Show alarm template names.

Syntax:

profile line-alarm-profile show alarm-template <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show line-alarm-profile

Description:

Show line alarm profile names.

Syntax:

profile line-alarm-profile show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show port

Description:

Show profile used in each port.

Syntax:

profile line-alarm-profile show port

profile line-alarm-profile show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile line-alarm-profile show virtual-noise <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile line-alarm-profile show dpbopsd <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile line-alarm-profile show rfi-bands <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile line-alarm-profile show psd <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile new**Description:**

Create new xDSL alarm profile.

Syntax:

profile line-alarm-profile new <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile del**Description:**

Delete xDSL alarm profile.

Syntax:

profile line-alarm-profile del <NAME>

Parameters:

<Name> profile name

profile line-alarm-profile set xtucFecs**Description:**

A threshold for the Fecs counter in the current 15M interval on XTU. Indicates that the FEC seconds threshold has been reached / exceeded for the referred xTU-C.

Syntax:

profile line-alarm-profile set xtucFecs <NAME><VALUE>

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xtucEs**Description:**

A threshold for the Es counter in the current 15M interval on XTUC. Indicates that the errored second threshold has been reached / exceeded for the referred xTU-C.

Syntax:

profile line-alarm-profile set xtucEs <NAME><VALUE>

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xtucSes**Description:**

A threshold for the Ses counter in the current 15M interval on XTUC. Indicates that the severely errored second threshold has been reached / exceeded for the referred xTU-C.

Syntax:

```
profile line-alarm-profile set xtucSes <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xtucLoss**Description:**

A threshold for the Loss counter in the current 15M interval on XTUC. Indicates that the LOS seconds threshold has been reached / exceeded for the referred xTU-C.

Syntax:

```
profile line-alarm-profile set xtucLoss <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xtucUas**Description:**

A threshold for the Uas counter in the current 15M interval on XTUC. Indicates that the unavailable second threshold has been reached / exceeded for the referred xTU-C.

Syntax:

```
profile line-alarm-profile set xtucUas <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xturFecs**Description:**

A threshold for the Fecs counter in the current 15M interval on XTUR.

Syntax:

```
profile line-alarm-profile set xturFecs <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xturEs**Description:**

A threshold for the Es counter in the current 15M interval on XTUR.

Syntax:

```
profile line-alarm-profile set xturEs <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xtucSes**Description:**

A threshold for the Ses counter in the current 15M interval on XTUR.

Syntax:

```
profile line-alarm-profile set xtucSes <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xturLoss**Description:**

A threshold for the Loss counter in the current 15M interval on XTUR.

Syntax:

```
profile line-alarm-profile set xturLoss <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set xturUas**Description:**

A threshold for the Uas counter in the current 15M interval on XTUR.

Syntax:

```
profile line-alarm-profile set xturUas <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set fullInt

Description:

A threshold for the count of failed full initializations in the current 15M interval. Indicates that the failed full initializations threshold has been reached / exceeded for the referred VDSL2 line.

Syntax:

```
profile line-alarm-profile set fullInt <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile line-alarm-profile set shrtInt

Description:

A threshold for the count of failed short initializations in the current 15M interval. Indicates that the failed short initializations threshold has been reached / exceeded for the referred VDSL2 line.

Syntax:

```
profile line-alarm-profile set shrtInt <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value

profile chan-alarm-profile show

Description:

Show all profile names or show detail information of a specified profile.

Syntax:

```
profile chan-alarm-profile line-template show
```

profile chan-alarm-profile show sprofile

Description:

Show system profile names.

Syntax:

```
profile chan-alarm-profile show sprofile
```

```
Switch(config)# profile chan-alarm-profile show sprofile
```

```
CO_Default
```

```
CPE_Default
```

```
A_R_POTS_D-32_EU-32
```

```
A_R_POTS_D-64_EU-64
```

```
B7-1_997-M1c-A-7
```

```
B7-2_997-M1x-M-8
```

```
B7-3_997-M1x-M
```

```
B7-4_997-M2x-M-8
```

```
B7-5_997-M2x-A
```

```
B7-6_997-M2x-M
```

```
B7-7_HPE17-M1-NUS0
```

```
B7-8_HPE30-M1-NUS0
```

```
B7-9_997E17-M2x-A
```

```
B7-10_997E30-M2x-NUS0
```

```
B8-1_998-M1x-A
```

```
B8-2_998-M1x-B
```

```
B8-3_998-M1x-NUS0
```

```
B8-4_998-M2x-A
```

```
B8-5_998-M2x-M
```

```
B8-6_998-M2x-B
```

```
B8-7_998-M2x-NUS0
```

```
B8-8_998E17-M2x-NUS0
```

```
B8-9_998E17-M2x-NUS0-M
```

```
B8-10_998ADE17-M2x-NUS0-M
```

```
B8-11_998ADE17-M2x-A
```

```
B8-12_998ADE17-M2x-B
```

```
B8-13_998E30-M2x-NUS0
```

```
B8-14_998E30-M2x-NUS0-M
```

```
B8-15_998ADE30-M2x-NUS0-M
```

```
B8-16_998ADE30-M2x-NUS0-A
```

```
C_POTS_25-138_b
```

```
C_POTS_25-276_b
```

```
C_TCM-ISDN
```

```
DEFVAL
```

```
CROSSTALK
```

```
VNS_WT115
```

```
DEFVAL
```

```
DEFVAL
```

```
WT115_GMDSS
```

```
WT115_TR100
```

```
WT115_ERUOPE
```

```
IN_993.2
```

```
DEFVAL
```

```
ANSI
```

```
EX_ANXI
```

```
ETSI
```

```
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#
```

profile chan-alarm-profile show line-template

Description:

Show line template names.

Syntax:

```
profile chan-alarm-profile show line-template <NAME>
```

Parameters:

<Name> profile name

profile chan-alarm-profile show line-profile

Description:

Show line profile names.

Syntax:

```
profile chan-alarm-profile show line-profile <NAME>
```

Parameters:

<Name> profile name

profile chan-alarm-profile show chan-profile

Description:

Show channel profile names.

Syntax:

```
profile chan-alarm-profile show chan -profile <NAME>
```

Parameters:

<Name> profile name

profile chan-alarm-profile show alarm-template

Description:

Show line template names.

Syntax:

profile chan-alarm-profile show alarm-template <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile show line-alarm-profile

Description:

Show line profile names.

Syntax:

profile chan-alarm-profile show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile show port

Description:

Show profile used in each port.

Syntax:

profile chan-alarm-profile show port

profile chan-alarm-profile show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile chan-alarm-profile show virtual-noise <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile chan-alarm-profile show dpbopsd <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile chan-alarm-profile show rfi-bands <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile chan-alarm-profile show psd <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile new

Description:

Create new xDSL channel alarm profile

Syntax:

profile chan-alarm-profile new <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile del

Description:

delete xDSL channel alarm profile.

Syntax:

profile chan-alarm-profile del <NAME>

Parameters:

<Name> profile name

profile chan-alarm-profile set cvThresXtuc**Description:**

A threshold for the coding violation counter in the current 15M interval on XTUC.

Syntax:

```
profile chan-alarm-profile set cvThresXtuc <NAME><VALUE>
```

Parameters:

<NAME> Profile name configure value of dec.

<VALUE> Configure value

profile chan-alarm-profile set correctedThresXtuc**Description:**

A threshold for the corrected code word counter in the current 15M interval on XTUC.

Syntax:

```
profile chan-alarm-profile set correctedThresXtuc <NAME><VALUE>
```

Parameters:

<NAME> Profile nameconfigure value of dec.

<VALUE> Configure value

profile chan-alarm-profile set cvThresXtur**Description:**

A threshold for the coding violation counter in the current 15M interval on XTUR.

Syntax:

```
profile chan-alarm-profile set cvThresXtur <NAME><VALUE>
```

Parameters:

<NAME> Profile nameconfigure value of dec.

<VALUE> Configure value

profile chan-alarm-profile set correctedThresXtur**Description:**

A threshold for the corrected code word counter in the current 15M interval on XTUR.

Syntax:

```
profile chan-alarm-profile set correctedThresXtur <NAME><VALUE>
```

Parameters:

<NAME> Profile name configure value of dec.

<VALUE> Configure value

profile pre-define

Description:

xDSL pre-define configuration.

Syntax:

```
profile pre-define
```

profile pre-define

Description:

A threshold for the corrected code word counter in the current 15M interval on XTUR.

Syntax:

```
profile pre-define [show | vn-new | vn-del | dep-new | dep-del | rfi-new | rfi-del | vn-det-ds | vn-set-us | dep-set |
rfi-set]
```

profile pre-define show

Description:

Show all profile names or show detail information of a specified profile.

Syntax:

```
profile pre-define show
```

profile pre-define show sprofile

Description:

Show system profile names.

Syntax:

```
profile pre-define show sprofile
```

```
Switch(config)# profile pre-define show sprofile
CO_Default
CPE_Default
A_R_POTS_D-32_EU-32
A_R_POTS_D-64_EU-64
B7-1_997-M1c-A-7
B7-2_997-M1x-M-8
B7-3_997-M1x-M
B7-4_997-M2x-M-8
B7-5_997-M2x-A
B7-6_997-M2x-M
B7-7_HPE17-M1-NUS0
B7-8_HPE30-M1-NUS0
B7-9_997E17-M2x-A
```

B7-10_997E30-M2x-NUS0
B8-1_998-M1x-A
B8-2_998-M1x-B
B8-3_998-M1x-NUS0
B8-4_998-M2x-A
B8-5_998-M2x-M
B8-6_998-M2x-B
B8-7_998-M2x-NUS0
B8-8_998E17-M2x-NUS0
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#

profile pre-define show line-template

Description:

Show line template names.

Syntax:

```
profile pre-define show line-template <NAME>
```

Parameters:

<Name> profile name

profile pre-define show line-profile

Description:

Show line profile names.

Syntax:

```
profile pre-define show line-profile <NAME>
```

Parameters:

<Name> profile name

profile pre-define show chan-profile

Description:

Show channel profile names.

Syntax:

```
profile pre-define show chan -profile <NAME>
```

Parameters:

<Name> profile name

profile pre-define show alarm-template

Description:

Show line template names.

Syntax:

```
profile pre-define show alarm-template <NAME>
```

Parameters:

<Name> profile name

profile pre-define show line-alarm-profile

Description:

Show line profile names.

Syntax:

```
profile pre-define show line-alarm-profile <NAME>
```

Parameters:

<Name> profile name

profile pre-define show port

Description:

Show profile used in each port.

Syntax:

```
profile pre-define show port
```

profile pre-define show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

```
profile pre-define show virtual-noise <NAME>
```

Parameters:

<Name> profile name

profile pre-define show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

```
profile pre-define show dpbopsd <NAME>
```

Parameters:

<Name> profile name

profile pre-define show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

```
profile pre-define show rfi-bands <NAME>
```

Parameters:

<Name> profile name

profile pre-define show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile pre-define show psd <NAME>

Parameters:

<Name> profile name

profile pre-define vn-new

Description:

Create new xdsl virtual noise psd profile.

Syntax:

profile pre-define vn-new <NAME>

Parameters:

<Name> profile name

profile pre-define vn-del

Description:

Delete xdsl virtual noise psd profile.

Syntax:

profile pre-define vn-del <NAME>

Parameters:

<Name> profile name

profile pre-define dep-new

Description:

Create new xdsl DpboEPsd profile.

Syntax:

profile pre-define dep-new <NAME>

Parameters:

<Name> profile name

profile pre-define dep-del**Description:**

Delete xdsl DpboEPsd profile.

Syntax:

profile pre-define dep-del <NAME>

Parameters:

<Name> profile name

profile pre-define rfi-new**Description:**

Create new xdsl RfiBands profile.

Syntax:

profile pre-define rfi-new <NAME>

Parameters:

<Name> profile name

profile pre-define rfi-del**Description:**

Delete xdsl RfiBands profile.

Syntax:

profile pre-define rfi-del <NAME>

Parameters:

<Name> profile name

profile pre-define vn-set-ds**Description:**

Set xdsl vitrual noise downstream psd profile.

Syntax:

profile pre-define vn-set-ds <NAME>

profile pre-define vn-set-ds <NAME> <INDEX><1-1700><NLEVEL>

Parameters:

<Name> profile name

<INDEX> index vn-set-ds:1~32; vn-set-us:1~16; dep-set:1~32.

<1-1700> Tone:1~7000(4.3125kHz)

<NLEVEL> Nlevel:-127.5~0dBm/Hz

profile pre-define vn-set-us

Description:

Set xdsl vitrual noise upstream psd profile.

Syntax:

```
profile pre-define vn-set-us <NAME>
profile pre-define vn-set-us <NAME> <INDEX><1-1700><NLEVEL>
```

Parameters:

<Name> profile name

<INDEX> index vn-set-ds:1~32; vn-set-us:1~16; dep-set:1~32.

<1-1700> Tone:1~7000(4.3125kHz)

<NLEVEL> Nlevel:-127.5~0dBm/Hz

profile pre-define dep-set

Description:

Set xdsl DpboPsd profile.

Syntax:

```
profile pre-define dep-set <NAME>
profile pre-define dep-set <NAME> <INDEX><1-1700><NLEVEL>
```

Parameters:

<Name> profile name

<INDEX> index vn-set-ds:1~32; vn-set-us:1~16; dep-set:1~32.

<1-1700> Tone:1~7000(4.3125kHz)

<NLEVEL> Nlevel:-127.5~0dBm/Hz

profile pre-define rfi-set

Description:

Set xdsl RfiBands profile.

Syntax:

```
profile pre-define rfi-set <NAME>
profile pre-define rfi-set <NAME><1-16><INDEX><1-1700>
```

Parameters:

<Name> profile name

<1-16> index 1~16

<INDEX> index vn-set-ds:1~32; vn-set-us:1~16; dep-set:1~32.

<1-1700> Start Tone:1~7000(4.3125kHz)

<1-1700> End Tone:1~7000(4.3125kHz)

profile port

Description:

xDSL Port configuration.

Syntax:

profile port [show | initprofile | set]

profile port show

Description:

Show all profile names or show detail information of a specified profile.

Syntax:

profile port show

profile port show sprofile

Description:

Show system profile names.

Syntax:

profile port show sprofile

```
Switch(config)# profile port show sprofile
```

```
CO_Default
```

```
CPE_Default
```

```
A_R_POTS_D-32_EU-32
```

```
A_R_POTS_D-64_EU-64
```

```
B7-1_997-M1c-A-7
```

```
B7-2_997-M1x-M-8
```

```
B7-3_997-M1x-M
```

```
B7-4_997-M2x-M-8
```

```
B7-5_997-M2x-A
```

```
B7-6_997-M2x-M
```

```
B7-7_HPE17-M1-NUS0
```

```
B7-8_HPE30-M1-NUS0
```

```
B7-9_997E17-M2x-A
```

```
B7-10_997E30-M2x-NUS0
```

```
B8-1_998-M1x-A
```

```
B8-2_998-M1x-B
```

```
B8-3_998-M1x-NUS0
```

```
B8-4_998-M2x-A
```

```
B8-5_998-M2x-M
```

```
B8-6_998-M2x-B
```

```
B8-7_998-M2x-NUS0
```

```
B8-8_998E17-M2x-NUS0
```

```
B8-9_998E17-M2x-NUS0-M
B8-10_998ADE17-M2x-NUS0-M
B8-11_998ADE17-M2x-A
B8-12_998ADE17-M2x-B
B8-13_998E30-M2x-NUS0
B8-14_998E30-M2x-NUS0-M
B8-15_998ADE30-M2x-NUS0-M
B8-16_998ADE30-M2x-NUS0-A
C_POTS_25-138_b
C_POTS_25-276_b
C_TCM-ISDN
DEFVAL
CROSSTALK
VNS_WT115
DEFVAL
DEFVAL
WT115_GMDSS
WT115_TR100
WT115_ERUOPE
IN_993.2
DEFVAL
ANSI
EX_ANXI
ETSI
EX_ETSI
PLAT
ADSL2PLUS
CO
DT
Switch(config)#
```

profile port show line-template

Description:

Show line template names.

Syntax:

```
profile port show line-template <NAME>
```

Parameters:

<Name> profile name

profile port show line-profile

Description:

Show line profile names.

Syntax:

profile port show line-profile <NAME>

Parameters:

<Name> profile name

profile port show chan-profile

Description:

Show channel profile names.

Syntax:

profile port show chan -profile <NAME>

Parameters:

<Name> profile name

profile port show alarm-template

Description:

Show line template names.

Syntax:

profile port show alarm-template <NAME>

Parameters:

<Name> profile name

profile port show line-alarm-profile

Description:

Show line profile names.

Syntax:

profile port show line-alarm-profile <NAME>

Parameters:

<Name> profile name

profile port show port

Description:

Show profile used in each port.

Syntax:

profile port show port

profile port show virtual-noise

Description:

Show single virtual noise line profile content.

Syntax:

profile port show virtual-noise <NAME>

Parameters:

<Name> profile name

profile port show dpbopsd

Description:

Show single DpboPsd line profile content.

Syntax:

profile port show dpbopsd <NAME>

Parameters:

<Name> profile name

profile port show rfi-bands

Description:

Show single RfiBands line profile content.

Syntax:

profile port show rfi-bands <NAME>

Parameters:

<Name> profile name

profile port show psd

Description:

Show single PsdMask line profile content.

Syntax:

profile port show psd <NAME>

Parameters:

<Name> profile name

profile port initprofile

Description:

Initialize profile to all vdsl port.

Syntax:

profile port initprofile

profile port set

Description:

Set commands for xdsl port.

Syntax:

profile port set <line-template | alarm-template>

Parameters:

<line-template> Apply VDSL line configuration template for this line.

<alarm-template> Apply VDSL line alarm configuration template for this line.

profile port set line-template

Description:

Apply VDSL line configuration template for this line.

Syntax:

profile port line-template <PORT><NAME>

Parameters:

<PORT> Port Number.

<NAME> Vdsl config Template Name.

profile port set alarm-template

Description:

Apply VDSL line alarm configuration template for this line.

Syntax:

profile port alarm -template <PORT><NAME>

Parameters:

<PORT> Port Number.

<NAME> Vdsl config Template Name.

profile chan-profile

Description:

Commands for xDSL channel configuration profile.

Syntax:

profile chan-profile [new | del | set]

Parameters:

<new> Create new xDSL channel configuration profile

 delete xDSL channel configuration profil

<set> set xDSL channel configuration profile

profile chan-profile new

Description:

Create new xDSL channel configuration profile.

Syntax:

profile chan-profile new <NAME>

Parameters:

<NAME> Profile name

profile chan-profile del

Description:

Delete xDSL channel configuration profile.

Syntax:

profile chan-profile del <NAME>

Parameters:

<NAME> Profile name

profile chan-profile set

Description:

Set xDSL channel configuration profile.

Syntax:

profile chan-profile set

profile chan-profile set minDataRateDsCh1

Description:

CH1 Mini Data Rate at DS, value range is 0~200000, unit is kbps.

Syntax:

```
profile chan-profile set minDataRateDsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set minDataRateUsCh1

Description:

CH1 Mini Data Rate at US, value range is 0~200000, unit is kbps.

Syntax:

```
profile chan-profile set minDataRateUsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set maxDataRateDsCh1

Description:

CH1 Maxi Data Rate at DS, value range is 0~200000, unit is kbps.

Syntax:

```
profile chan-profile set maxDataRateDsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set maxDataRateUsCh1

Description:

CH1 Maxi Data Rate at US, value range is 0~200000, unit is kbps.

Syntax:

```
profile chan-profile set maxDataRateUsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set maxDelayDsCh1

Description:

CH1 Max Interleave Delay at DS,value range is 0~255, unit is ms.

Syntax:

```
profile chan-profile set maxDelayDsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set maxDelayUsCh1

Description:

CH1 Max Interleave Delay at US,value range is 0~255, unit is ms.

Syntax:

```
profile chan-profile set maxDelayUsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set minInpDsCh1

Description:

CH1 DS min INP in 4.3125kHz, value range is 1-18.

Syntax:

```
profile chan-profile set minInpDsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set minInpUsCh1

Description:

CH1 US min INP in 4.3125kHz, value range is 1-18.

Syntax:

```
profile chan-profile set minInpUsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set minInp8DsCh1

Description:

CH1 DS min INP in 8.625kHz, value range is 1-17.

Syntax:

```
profile chan-profile set minInp8DsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

profile chan-profile set minInp8UsCh1

Description:

CH1 US min INP in 8.625kHz, value range is 1-17.

Syntax:

```
profile chan-profile set minInp8UsCh1 <NAME><VALUE>
```

Parameters:

<NAME> Profile name

<VALUE> Configure value.

7. Layer 2 OPERATION

7.1 Address Table

The IP DSLAM is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Switch.

7.2 Learning

When one packet comes in from any port, the IP DSLAM will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The IP DSLAM scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the IP DSLAM attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the IP DSLAM is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters. Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The IP DSLAM performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the IP DSLAM have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)
1000Mbps, with auto-negotiation	1000/2000Mbps (1000Base-T/Full-Duplex)

8. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the Ethernet DSLAM is not functioning properly, make sure the IP DSLAM was set up according to instructions in this manual.

■ The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the IP DSLAM

■ Some stations cannot talk to other stations located on the other port

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ Performance is bad

Solution:

Check the full duplex status of the IP DSLAM. If the IP DSLAM is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ Why the IP DSLAM doesn't connect to the network

Solution:

1. Check the LNK/ACT LED on the IP DSLAM
2. Try another port on the IP DSLAM
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ 100Base-TX port link LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software DSLAM to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

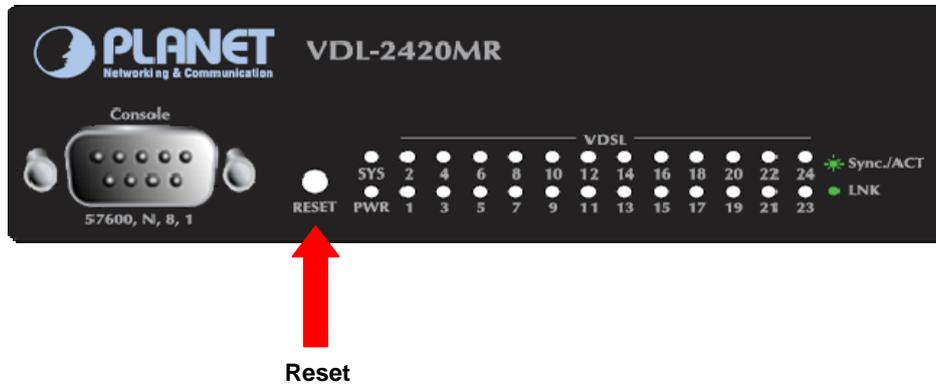
■ DSLAM does not power up

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord if the cord is inserted correctly; check that the AC power source is working by connecting a different device in place of the IP DSLAM.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

■ While IP Address be changed or forgotten admin password –

To reset the IP address to the default IP Address "192.168.0.100" or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds**. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDIX A—RJ-45 Pin Assignment

A.1 DSLAM's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

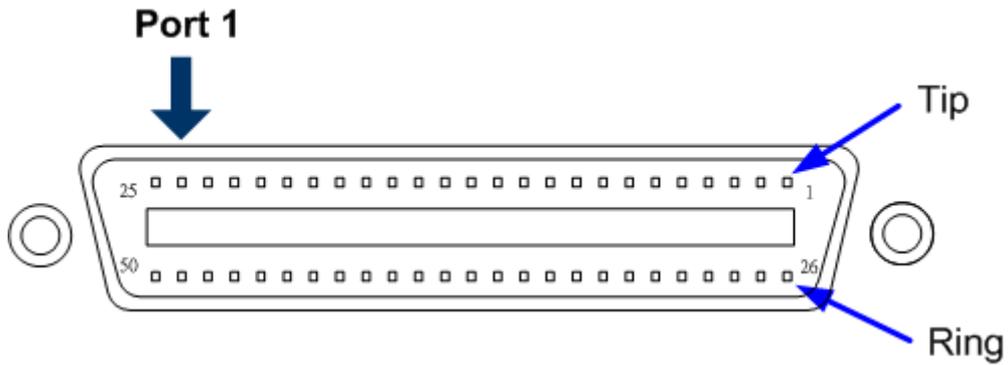
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet DSLAM to another DSLAM, a bridge or a hub, a straight or crossover cable is necessary. Each port of the IP DSLAM supports auto-MDI/MDI-X detection. That means you can directly connect the IP DSLAM to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

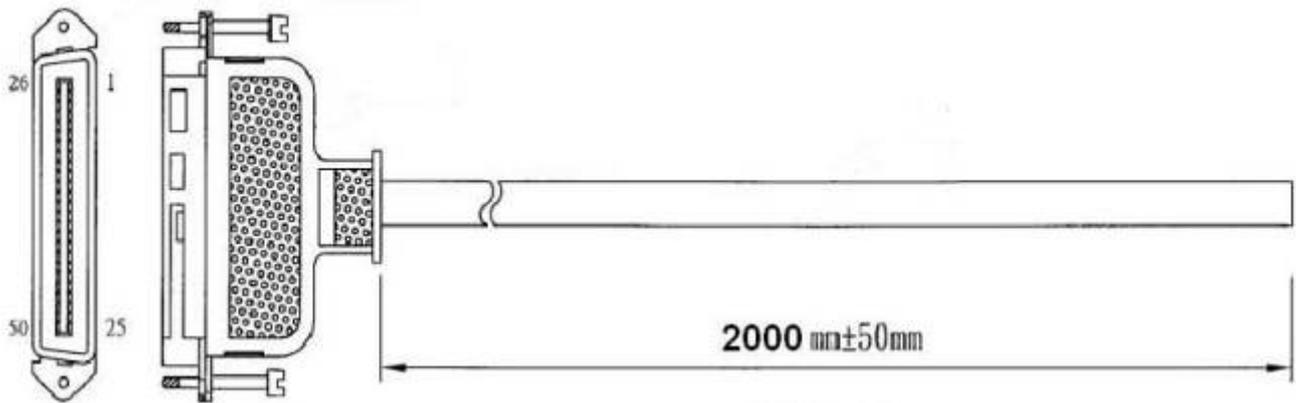
A.3 RJ-21 Connector pin out for VDL-2420MR Series



The above picture is the RJ-21 connector on VDL-2420MR series. The following lists the RJ-21 connector pin outs:

Pin	Port / Function	Pin	Port / Function
1	Port 24, Tip	26	Port 24, Ring
2	Port 23, Tip	27	Port 23, Ring
3	Port 22, Tip	28	Port 22, Ring
4	Port 21, Tip	29	Port 21, Ring
5	Port 20, Tip	30	Port 20, Ring
6	Port 19, Tip	31	Port 19, Ring
7	Port 18, Tip	32	Port 18, Ring
8	Port 17, Tip	33	Port 17, Ring
9	Port 16, Tip	34	Port 16, Ring
10	Port 15, Tip	35	Port 15, Ring
11	Port 14, Tip	36	Port 14, Ring
12	Port 13, Tip	37	Port 13, Ring
13	Port 12, Tip	38	Port 12, Ring
14	Port 11, Tip	39	Port 11, Ring
15	Port 10, Tip	40	Port 10, Ring
16	Port 9, Tip	41	Port 9, Ring
17	Port 8, Tip	42	Port 8, Ring
18	Port 7, Tip	43	Port 7, Ring
19	Port 6, Tip	44	Port 6, Ring
20	Port 5, Tip	45	Port 5, Ring
21	Port 4, Tip	46	Port 4, Ring
22	Port 3, Tip	47	Port 3, Ring
23	Port 2, Tip	48	Port 2, Ring
24	Port 1, Tip	49	Port 1, Ring
25	No Connect	50	No Connect

A.4 RJ-21 / Telco 50 Cable pin out



Port-24



Connector PIN	1	2	3	4	5	6	7	8	9
Wire Color	Blue	Orange	Green	Brown	Grey	Blue	Orange	Green	Brown
Connector PIN	26	27	28	29	30	31	32	33	34
Wire Color	White	White	White	White	White	Red	Red	Red	Red

Connector PIN	10	11	12	13	14	15	16	17	18
Wire Color	Grey	Blue	Orange	Green	Brown	Grey	Blue	Orange	Green
Connector PIN	35	36	37	38	39	40	41	42	43
Wire Color	Red	Black	Black	Black	Black	Black	Yellow	Yellow	Yellow

Connector PIN	19	20	21	22	23	24	25
Wire Color	Brown	Grey	Blue	Orange	Green	Brown	Grey
Connector PIN	44	45	46	47	48	49	50
Wire Color	Yellow	Yellow	Purple	Purple	Purple	Purple	Purple



Port-1

EC Declaration of Conformity

For the following equipment:

*Type of Product : 24-Port VDSL2 IP DSLAM
*Model Number : VDL-2420MR / VDL-2420MR48
* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address : 11F, No. 96, Min Chuan Road, Hsin Tien,
Taipei, Taiwan, R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).

For the evaluation regarding the EMC, the following standards were applied:

Emission	EN 55022	(2006)
Harmonic	EN 61000-3-2	(2006)
Flicker	EN 61000-3-3	(1995 + A1:2001 + A2:2005)
Immunity	EN 55024	(1998 + A1:2001 + A2:2003)
ESD	IEC 61000-4-2	(1995 + A1:1998 + A2:2000)
RS	IEC 61000-4-3	(2006)
EFT/ Burst	IEC 61000-4-4	(2004)
Surge	IEC 61000-4-5	(2005)
CS	IEC 61000-4-6	(2007)
Magnetic Field	IEC 61000-4-8	(1993 + A1:2000)
Voltage Disp	IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

Manufacturer Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan
Place

13th, Aug. 2010
Date


Legal Signature

PLANET TECHNOLOGY CORPORATION